

Azimuth User Manual - 2015



Document No _____ Rev _____

Uncontrolled Copy

☐

Controlled Copy

☐

Date _____

COMPANY PROPRIETARY INFORMATION

Prior to use, ensure this document is the most recent revision by checking the Master Document List. To request a change, submit a Document Change Request to the Document Control Representative.

Table of Contents.

TABLE OF CONTENTS.....	2
INTRODUCTION.	3
1.0 AN INTRODUCTION TO AZIMUTH.	3
2.0 AZIMUTH HARDWARE.	3
3.0 AZIMUTH SCREEN LAYOUT.....	5
4.0 CONNECTING CAMERAS.	7
5.0 CAMERA SWITCHERS.	13
6.0 THE “MAN-MACHINE INTERFACE”.	15
7.0 MOTION DETECTION SETTINGS.....	18
8.0 MAPPING.	22
9.0 iDIGITAL SETUP.	24
10.0 SETTING UP PATROLS.....	27
11.0 TRACK AND ZOOM.	29
12.0 VSAAS SETUP.	31
13.0 CONNECTING TO AZIMUTH CLIENT.	33
14.0 MISCELLANEOUS.....	35
15.1 Setting up a Joystick.	43

Introduction.

Azimuth is copyright ©Azimuth Ltd 2015.

Merlin3 is copyright ©Initsys Ltd 2003 - 2015 and this copyright is exclusively licensed to Azimuth Ltd.

The rights to the software design and implementation of the Azimuth concept is copyright ©Christopher Berry 2003 – 2015 and is exclusively licensed to Azimuth Ltd.

Details.

The owner of this software claims all rights. All rights reserved.

You may not copy, distribute or use this software without the prior written permission of the copyright owners and Azimuth.

Ownership of this software remains with its copyright holder at all times.

This manual contains watermarking characters that identify the owner and this information will be used to trace the source in the event of an unauthorized copy being made and distributed.

1.0 An introduction to Azimuth.

*The word azimuth is derived from the Arabic **اسموت** ('as-sumūt') referring to the ways or directions a person faces.*

Azimuth is the latest recording software for IP cameras. Its design is unique being compatible with many of the world's IP camera manufacturers as well as compatibility with analogue cameras through a converter (video server).

Azimuth is built around the high reliability database "Maria" and is suitable for recording from just a handful of IP cameras to many hundreds.

Using a high speed codec and Maria database means that Azimuth is capable of handling CCTV systems of virtually any size and complexity. Images can be used to create alarms, events and to feed the Azimuth VerifiedAlarms network and Merlin3 our control room software. Merlin3 incorporates both traditional alarm monitoring but additionally the third dimension, video with audio. Ideally suited for the monitoring of intruder alarms with video verification as well as video surveillance via IP cameras, DVRs and other systems.

The Maria database used in Azimuth ensures that images are recorded safely and reliably and can be accessed by SQL queries. Systems of any size can be built as well as ultra-reliable clusters and extreme redundancy systems.

In larger systems images are processed and passed to Maria for storage, this allows front end processors to capture and analyze the images without the overhead of the database.

2.0 Azimuth hardware.

This sections describes the various recommended hardware options for Azimuth.

Azimuth can be configured to operate on a single machine (even a notebook) or multiple front end processors working with a centralized Maria database.

Ultimately it is your decision on how much or how little resource you allocate to Azimuth.

Details.

Azimuth is comprised of two types of software applications,

Azimuth FEP.

Azimuth Database: The Client is the operators' link to Azimuth this can then be put on a desktop computer, for best results to the operator the system should have dual display.

Recommended System Hardware:

IAF – Install and Forget

Components:

Intel i5 3.2Ghz

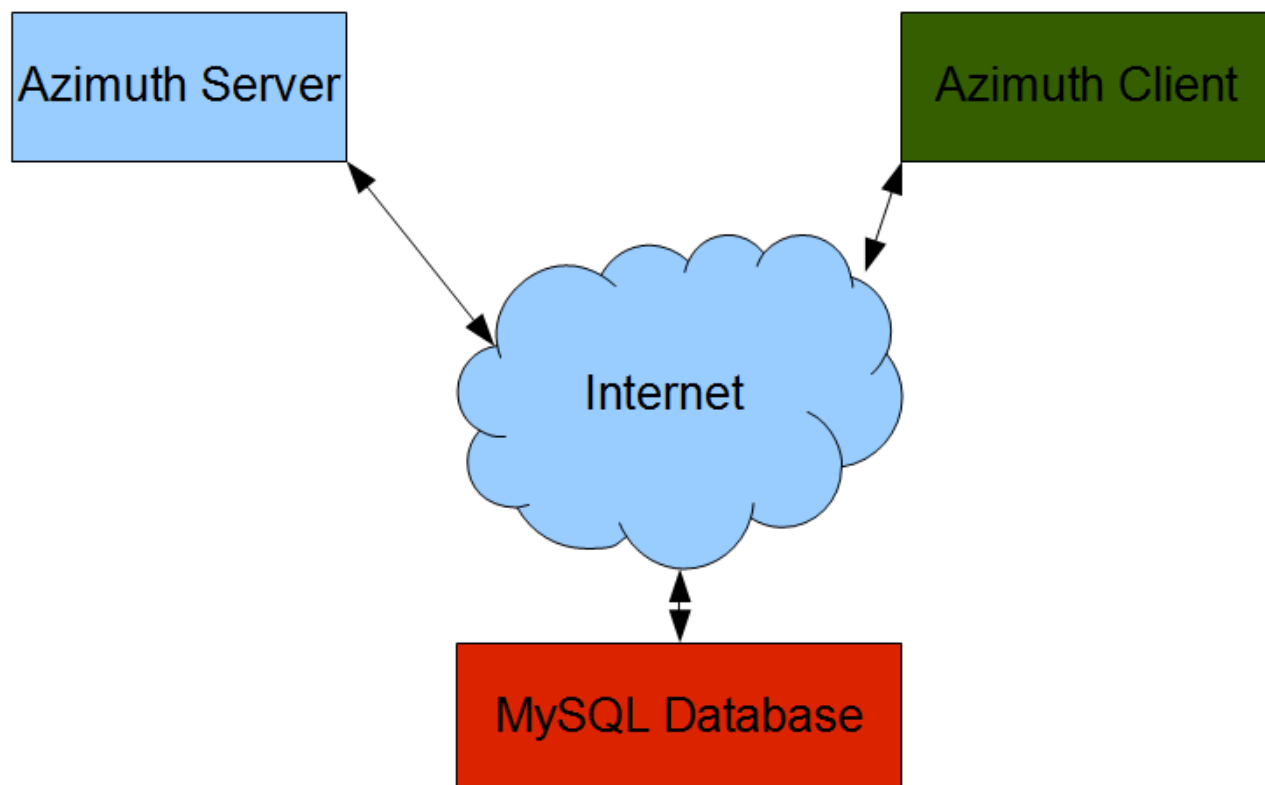
Windows Vista - Windows 8.1 / 32bit or 64bit

8GB SDRAM Memory

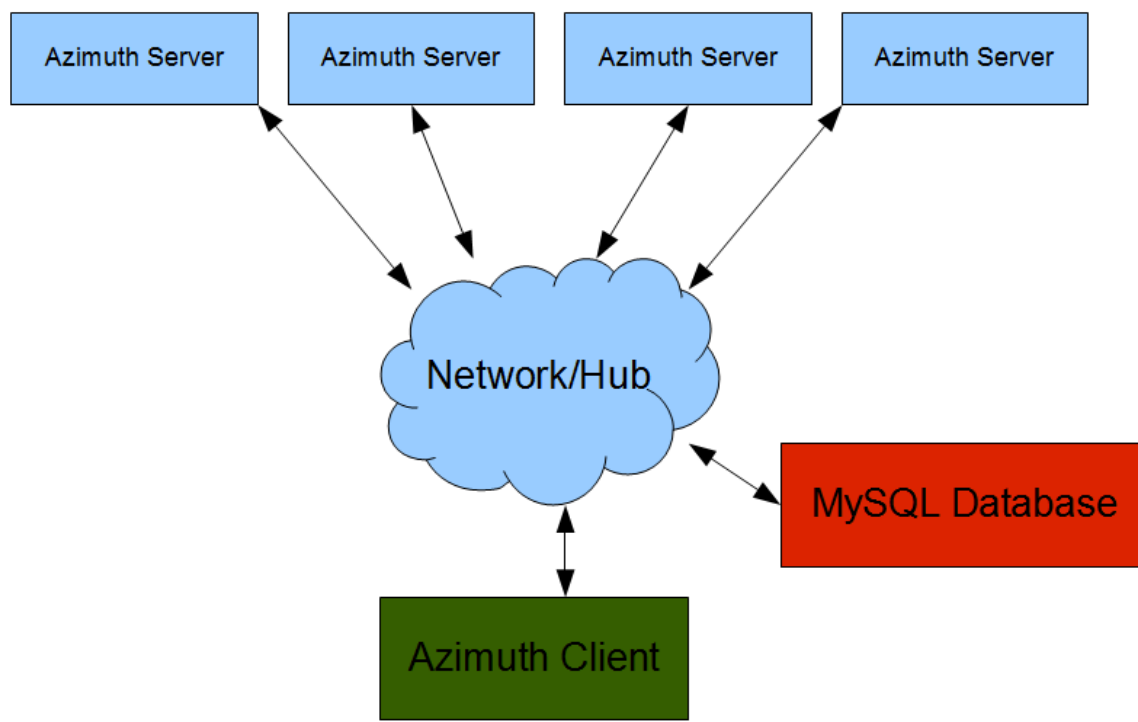
2TB+ Hard Drive

Example.

Here follows two diagrams showing how Azimuth can be used on a site.

Diagram

This diagram shows how Azimuth can be installed in one location, and monitored in another. In many instances Azimuth has been installed as a “Headless” unit, without monitors, keyboards, and mouse’s, with only an internet connection, allowing remote access via the Client for recordings or camera details. With use of a remote access program such as VNC a server can remain headless, with any changes to programming being made remotely. An independent Maria database is optional, but the preferred method is to have it on the Server machine. None of these different units need to be in the same location, the can be independent of each other.



The above diagram shows how multiple Azimuth servers can be installed to one location and viewed by one client either in the same location or elsewhere. Not only that, but the Client can view multiple Servers in a number of different locations, allowing company HQ's to monitor their locations. Again, the Maria Database being based elsewhere is entirely optional.

Maria: The Maria database program is a very powerful system, this now supports its own replication/clustering application. The hardware/software specifications are recommended by Maria and will not be given in this manual as they change quite frequently. However a basic cluster has been illustrated in the above diagram.

It shows the two types of applications

1. Maria Load Balancer – This application passes information about the database to and from the client, the client will see an IP address to connect to the load balancer which always remains the same, therefore if the load balancer is to drop out the spare load balancer would automatically take on its role.
2. Maria DataBase Node – This application is where the database is held, it can be replicated on a multiple amount of these nodes (yet it is not shared between them, so a full copy of the database is on each node), therefore if one where to drop out you will not lose data or will it disrupt Merlin's activity.

Clustering is an advantage in numerous ways, not only is it highly available and easy to maintain, it also reduces the lag between queries down to its load balancing techniques.

Also shown in the diagram is a branch off the cluster to the Disaster Recovery site. It is possible to replicate/cluster to an offsite location, which will make instant data recovery if you should ever need to switch to your DR location, it should also lower the need to remove backup copies of the database from your main location.

3.0 Azimuth Screen Layout.

Operational requirements dictate that images from the cameras are displayed for humans to view, and use. Careful thought has gone into Azimuth so that this is as flexible as possible.

The main screen comprises a top bar that gives access to all the main control features of the software, this enables the remainder of the screen to be devoted to the important CCTV images.

Under the menu list on the top of the screen are a series of LED's these are described below.

Left to Right

1. Sending Control Command.

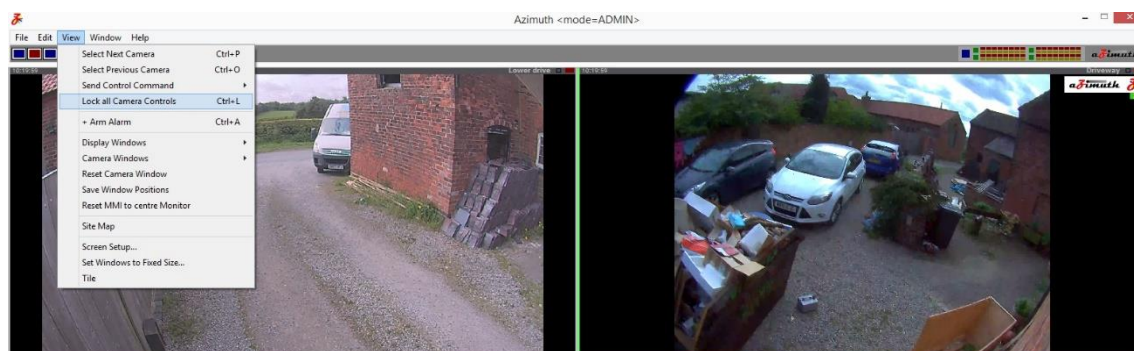
2. Access Mode.
3. Sending VerifiedAlarms alarm.
4. Sending Merlin Alarm.
5. Azimuth Audio Recording.
6. Remote Client Server.
7. Azimuth Communications Server.
8. Azimuth Web Server.
- 9.Verified Storage Status.



(Hovering the clicker over each of these options will indicate what their purpose is)

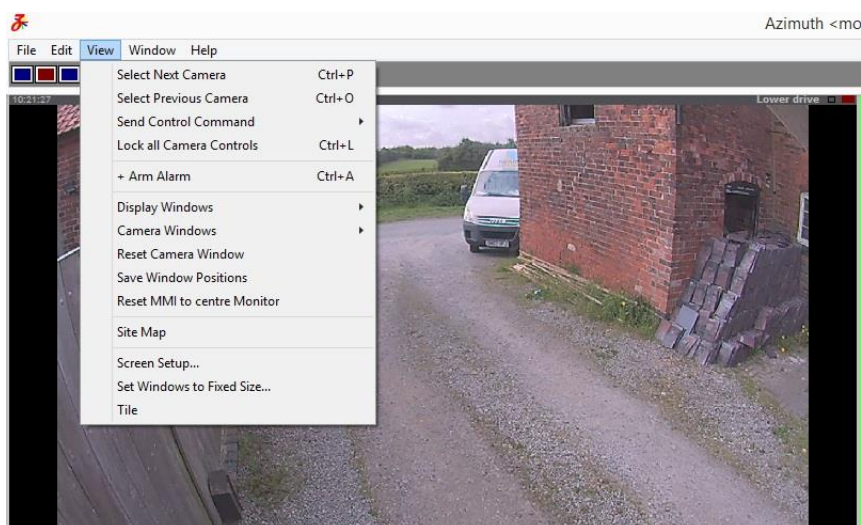
Details.

The Azimuth “pane” is the key to the flexibility of Azimuth. It is possible to move and position individual panes, hide them based on user privileges, resize them and just about do anything you want with them. Pane size is NOT dependent on the size of the frame you are recording.



The control of the panes is controlled through the “View” menu.

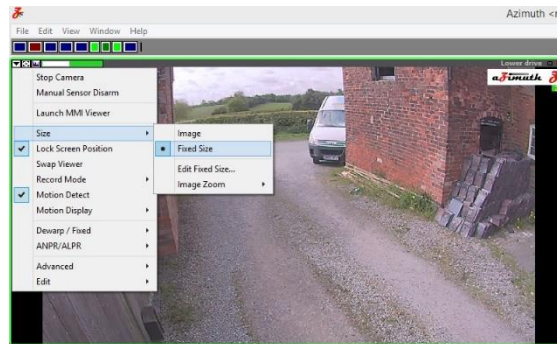
The top half of the View menu gives us control of individual cameras, the lower half control of the panes.



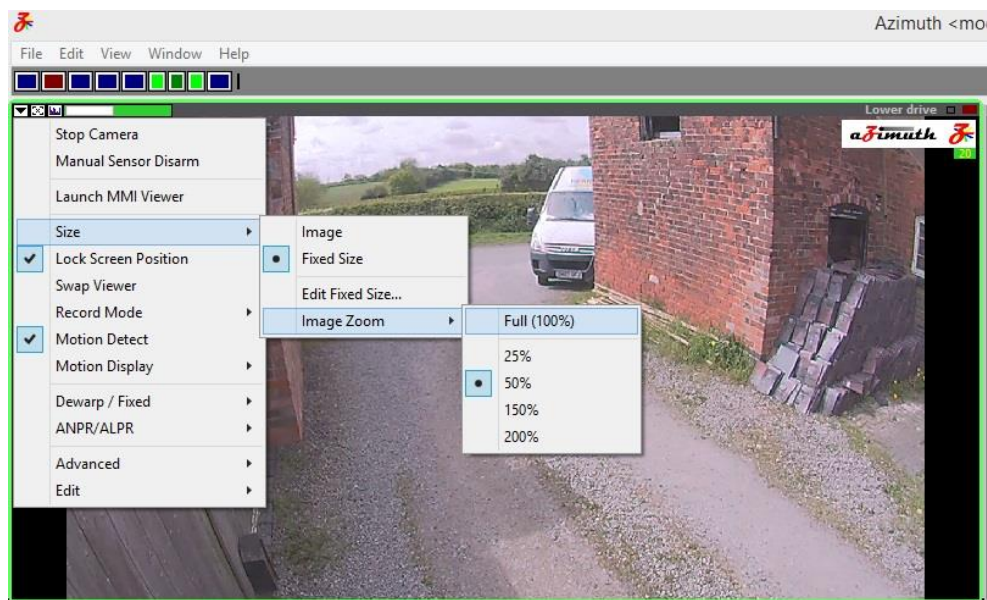
The view menu gives global control of the cameras and each pane has the same settings, allowing virtually unlimited design of the screen layout.

Panes can then be locked into position and to prevent alterations to the screen layout.

Example.



A Panes' position is controllable independently of the global settings.

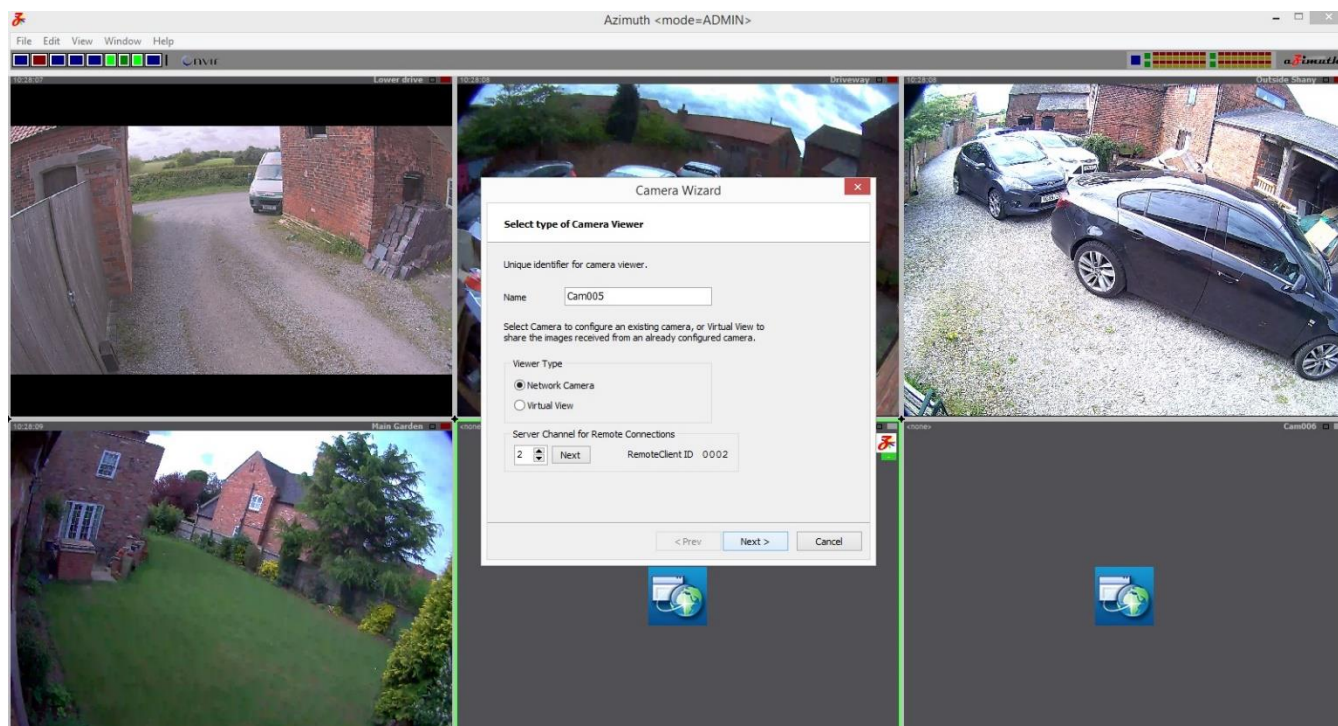


And the pane can be zoomed to a different size.

4.0 Connecting Cameras.

Adding cameras to Azimuth is very easy.

If you have created a screen layout using the option <Screen Setup> you will be presented with a number of windows that are “dummy”, on clicking the edit camera button you will be presented with the add camera wizard.



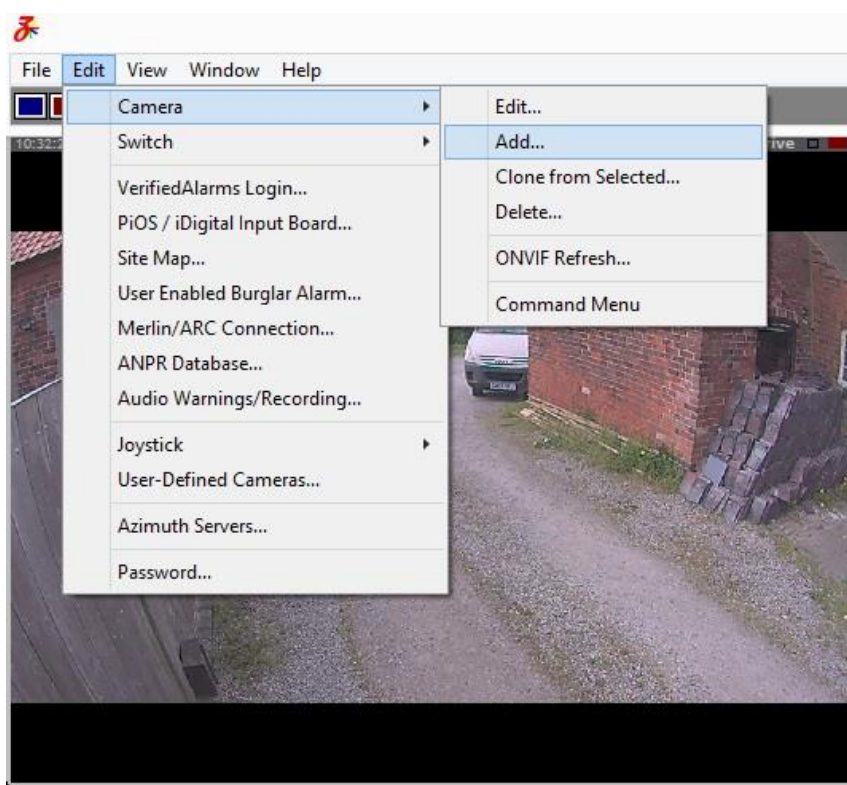
Simply follow the Add Camera Wizard to create your camera.

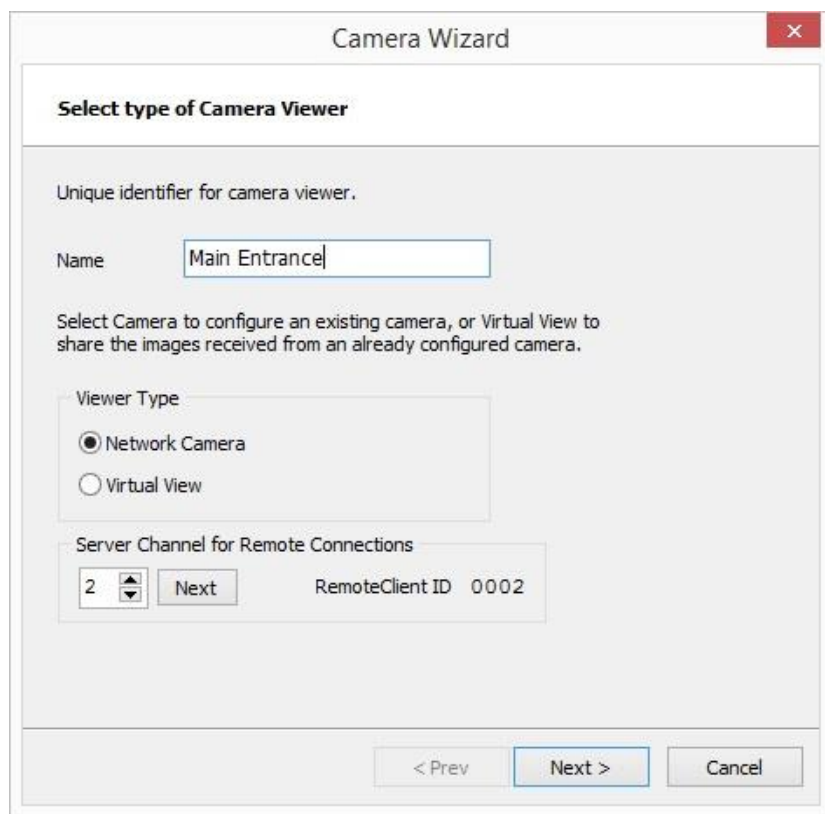
To manually configure a camera follow the process shown here.

Details.

Follow Edit → Camera → Add.

Camera wizard





Camera Wizard

Select type of Camera Viewer

Unique identifier for camera viewer.

Name

Select Camera to configure an existing camera, or Virtual View to share the images received from an already configured camera.

Viewer Type

☒ Network Camera

☐ Virtual View

Server Channel for Remote Connections

RemoteClient ID 0002

< Prev Next > Cancel

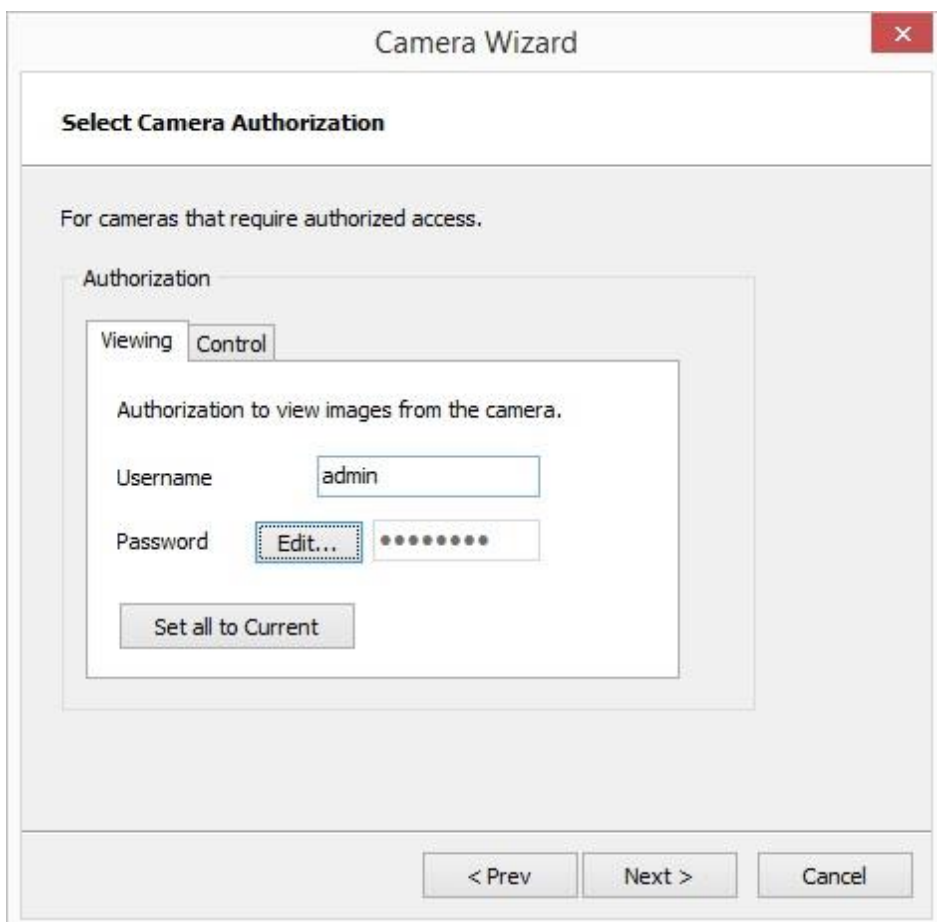
From Here you will be faced with a new window through which you will input all the cameras required details.

In this window you will be required to input Data (not always essential) into 10 different windows to allow Azimuth to bring the best from that particular type of camera that you are adding. If, for example, you are using a camera with PTZ capabilities Azimuth will need to know certain details in order for this feature to work at its full potential.

On the first page it asks for a name. This is simply what you would like the camera to be called, usually relating to its location ease of use to an operator when viewing a camera and gaining recorded footage. Below it asks for you to select whether it is a network camera or a client view, and finally what ID it will have for the remote Client (Azimuth Client).

Continue on to the next page. Select the Manufacturer of the camera, and that particular model, and input the cameras IP address and Port number (Should one be used, leave as default of 80 if not). Continue to the next page.

This page asks you for information regarding the cameras Authorization. There are three Username/Password combinations that Azimuth may require. The first is viewing, this is the username and password that is required for basic authorization allowing an operator to view the camera but little else. Control is a username and password required to authorize the operator to control the cameras PTZ functionality, and the final option is for the operator to be able to make changes to the cameras settings. If the camera is a simple static camera with few settings, only one password will be required, in which case simply input these details and select "Set all to Current" as this will assign the same details to each of the three sections, allowing the camera to be freed up. If more than one username and password is used for each section then the user must ensure each is input individually.



Camera Wizard

Select Camera Authorization

For cameras that require authorized access.

Authorization

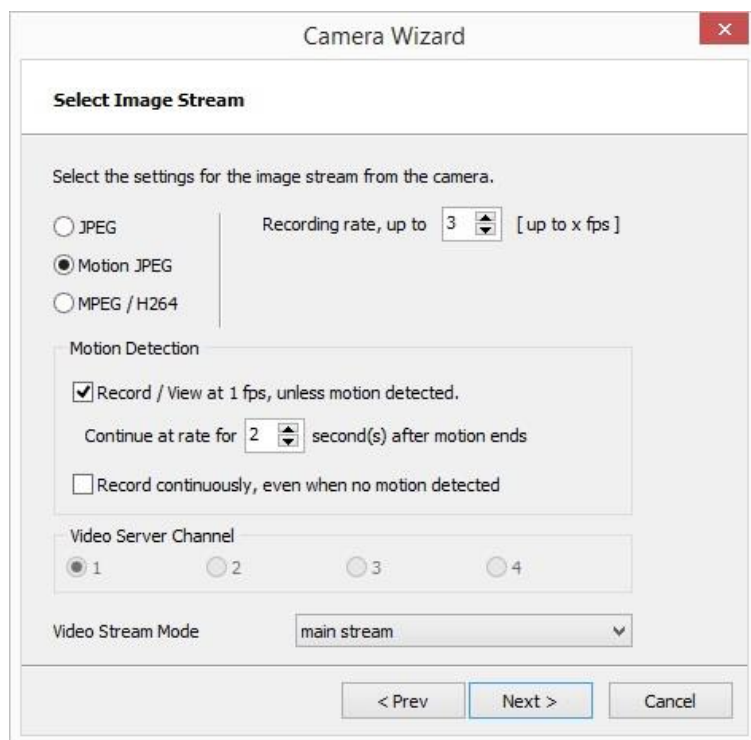
Viewing Control

Authorization to view images from the camera.

Username

Password

< Prev Next > Cancel



Camera Wizard

Select Image Stream

Select the settings for the image stream from the camera.

☐ JPEG
 ☒ Motion JPEG
 ☐ MPEG / H264

Recording rate, up to [up to x fps]

Motion Detection

☒ Record / View at 1 fps, unless motion detected.
 Continue at rate for second(s) after motion ends
☐ Record continuously, even when no motion detected

Video Server Channel

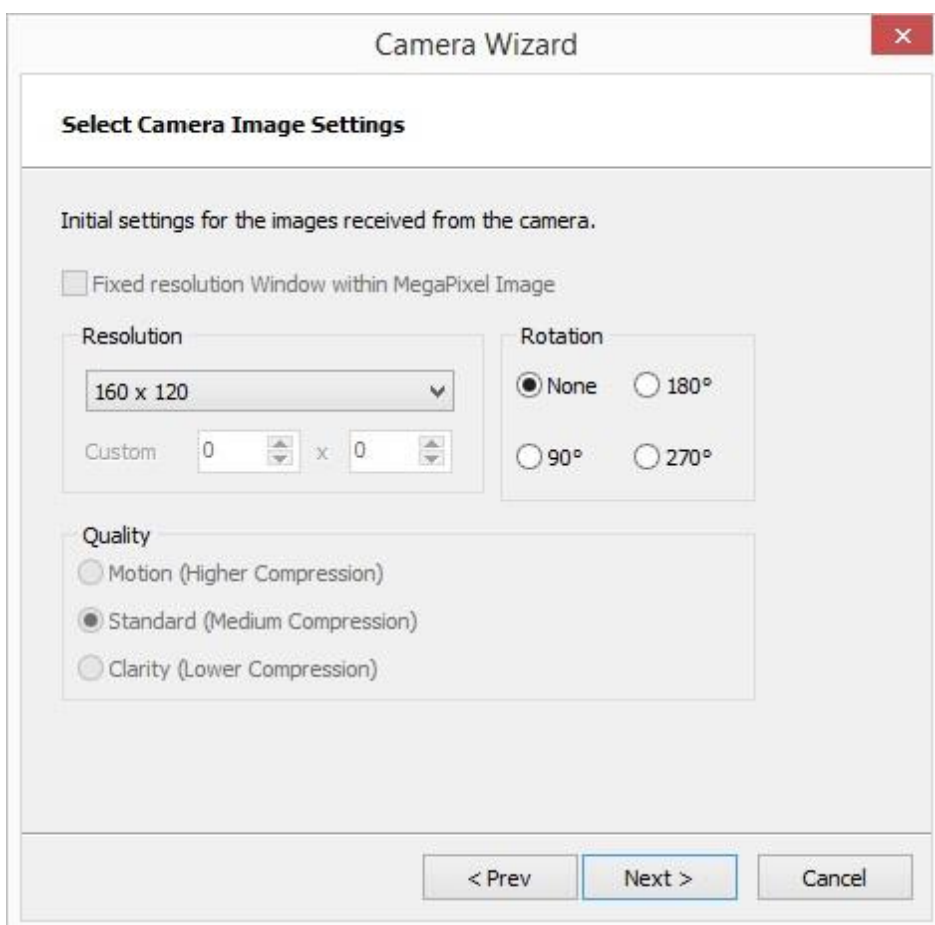
☒ 1
 ☐ 2
 ☐ 3
 ☐ 4

Video Stream Mode:

< Prev Next > Cancel

The next page is the Image Stream settings. Here you will be asked what frame rate the camera will stream at and what frame rate it will record at. It can also be used to determine whether or not the camera records at a different frame rate only when Motion is detected. Also present in this section is the ability to set the camera to constant record. At the very bottom of this page is an option to select which channel of a video server you wish to use. This section will automatically either be grayed out or be a usable option dependent on whether you have selected a Video server on page 2. Note that Azimuth will only make this a definable option should you input a video server with more than one channel. By selecting an individual channel the viewer will show that channel only, and cannot be used to show a multi-image view. In this particular case, Azimuth is aware that a Panasonic IP camera is being added, and therefore the option of a channel is not relevant.

The next page relates to your Image Settings. If for example due to installation restrictions a camera has been installed at an odd angle, it can be rotated so viewed correctly. The resolution relates to how large the viewer image is, this can be changed in a different section once set should it be required. The final option is image quality, and here you can define the quality of the image. It is of course worth noting that the higher the image quality, the more that is asked of the Computer and could compromise operating speeds, recording space, and how many cameras you are able to add. At the top of this window you will see an option that will only become available with the correct camera. This tickable box allows for the window to be resized so that it is an optimal size for a MegaPixel camera but by clicking this option you could A) Be faced with an image that you will never be able to see in its entirety, or B) Seriously decrease the Computers operating speed as it will assign all of its PCU usage into generating the MegaPixel image. It is recommended that you define what size you would like the image to be, it can still be recorded in its optimal size.



Camera Wizard

Select Camera Image Settings

Initial settings for the images received from the camera.

☐ Fixed resolution Window within MegaPixel Image

Resolution

x

Custom x

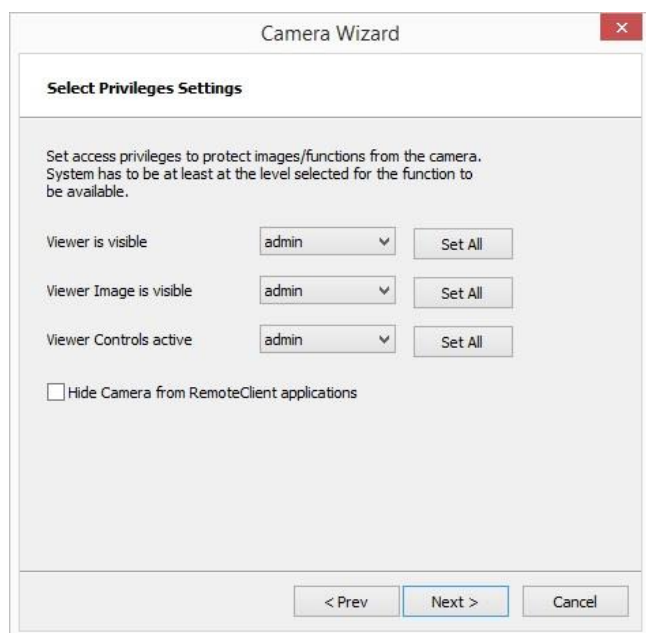
Rotation

☒ None
 ☐ 180°
☐ 90°
 ☐ 270°

Quality

☐ Motion (Higher Compression)
☒ Standard (Medium Compression)
☐ Clarity (Lower Compression)

< Prev Next > Cancel



Camera Wizard

Select Privileges Settings

Set access privileges to protect images/functions from the camera. System has to be at least at the level selected for the function to be available.

Viewer is visible: admin [v] Set All

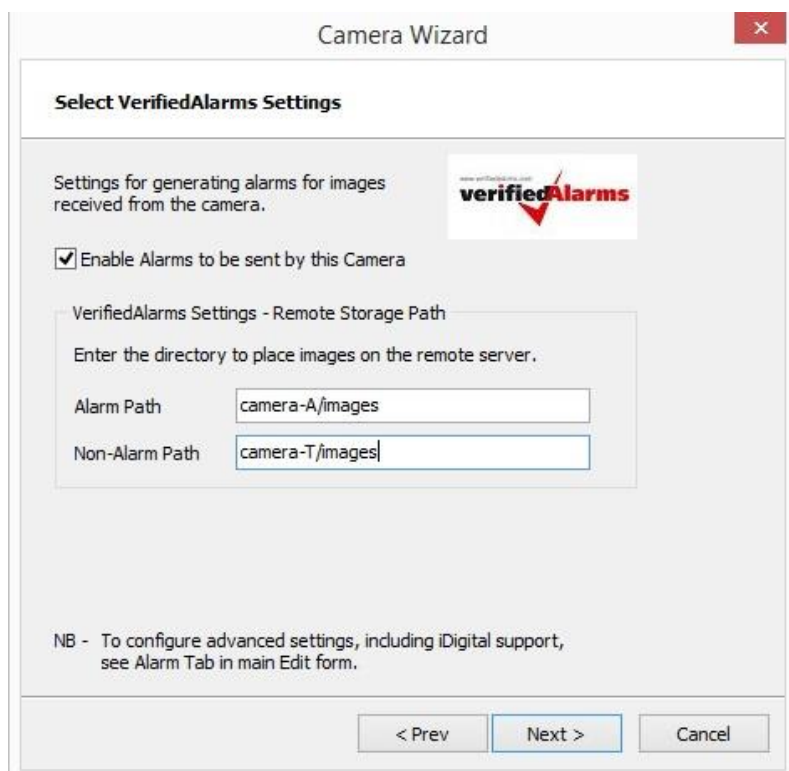
Viewer Image is visible: admin [v] Set All

Viewer Controls active: admin [v] Set All

☐ Hide Camera from RemoteClient applications

< Prev Next > Cancel

The next page is Camera Privileges. This section is where you determine what user levels can do what with the camera you're adding. "Viewer is Visible" means that the Viewer window itself will be visible to the operator, but that the actual camera image will not. "Viewer Image is Visible" means that the actual camera Image will become visible to the operator, and the final option will allow for the operator to perform PTZ functions and have control of where the camera is looking. Each option has a drop down box with 5 different user settings that can be determined elsewhere in the program. By selecting "None" you are enabling any user authorization to that function. If you wish for each of the three sections to have the same user settings, simply click on the option you wish to use in the drop down box and click "Set all" and all three sections will change. The final option in this window allows for you to hide the camera from the Remote Client (Azimuth Client) meaning that it will be visible on the Server Machine but will be non-existent as far as an operating user a client machine is concerned.



Camera Wizard

Select VerifiedAlarms Settings

Settings for generating alarms for images received from the camera.

☒ Enable Alarms to be sent by this Camera

VerifiedAlarms Settings - Remote Storage Path

Enter the directory to place images on the remote server.

Alarm Path: camera-A/images

Non-Alarm Path: camera-T/images

NB - To configure advanced settings, including iDigital support, see Alarm Tab in main Edit form.

< Prev Next > Cancel

The next page is where details relating to the cameras Verified Alarms settings will be input. If you have already generated a Verified Alarms page and added the camera, you will have had an alarm or none-alarm path created which you put into this section. This is all the information this part needs, and you will also have to click the option to enable the camera to send alarm images.

The next page allows for Images to be "Cached" for the purpose of FTP. This is so that pre and post alarm images can be sent to the FTP server. In this page simply select how many images will be cached as Pre-event images.



Camera Wizard

Select Recording Settings

Settings for folders required for functioning of Azimuth. For new cameras, initial default folders based on Camera Name setting will be automatically created, if not already existing.

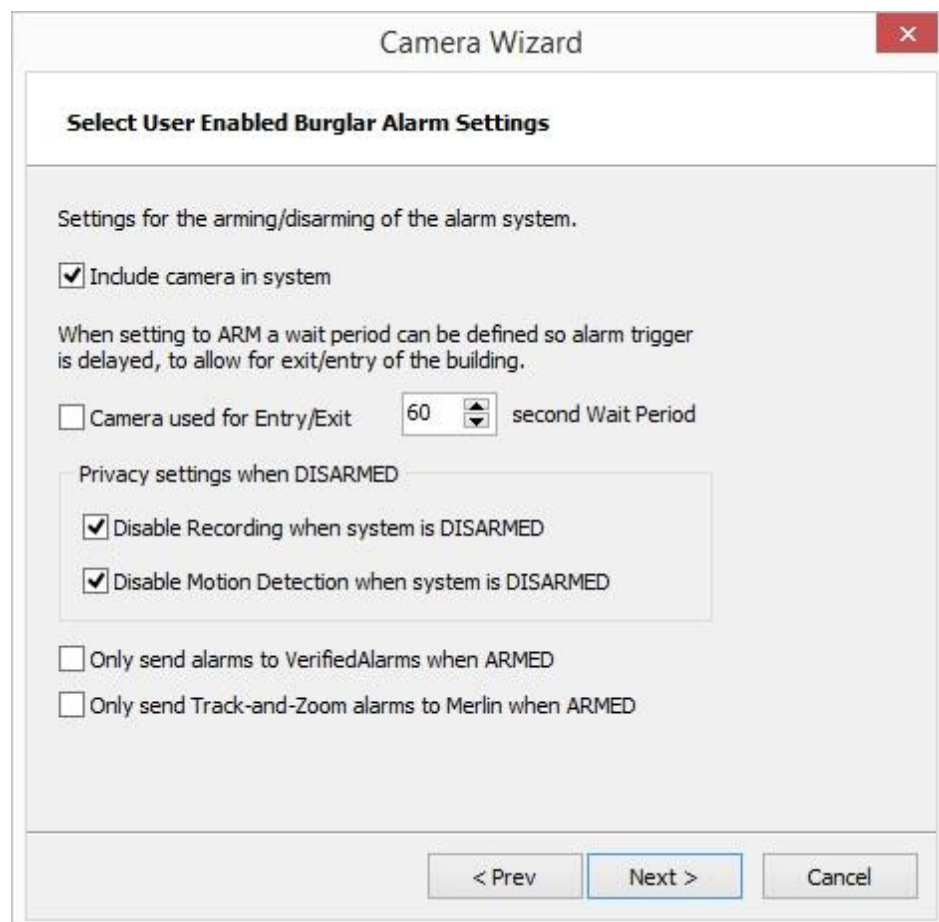
Local Alarm Cache

Alarm images will be temporarily stored before FTP to server. Set the Maximum temporary Files stored.

Cache Limit: 10 images [v]

NB - To configure advanced folder settings see Folders Tab in main Edit form.

< Prev Next > Cancel



Camera Wizard

Select User Enabled Burglar Alarm Settings

Settings for the arming/disarming of the alarm system.

☒ Include camera in system

When setting to ARM a wait period can be defined so alarm trigger is delayed, to allow for exit/entry of the building.

☐ Camera used for Entry/Exit 60 second Wait Period

Privacy settings when DISARMED

☒ Disable Recording when system is DISARMED

☒ Disable Motion Detection when system is DISARMED

☐ Only send alarms to VerifiedAlarms when ARMED

☐ Only send Track-and-Zoom alarms to Merlin when ARMED

< Prev Next > Cancel

The next page allows for options available with certain cameras to be used. Panasonic camera for example have outputs that can be used in order to Open doors, turn of lights, or arm an alarm system etc. Here you can define whether or not this camera is part of that system, select a delay time for when Outputs are used, and define what the camera does when Disarmed and Armed.

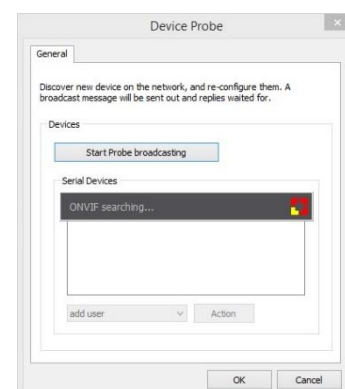
On the next page select finish, and the camera configuration is complete. If you fail to receive an image when the new window is added it could be for a number of options. You can retrace your steps in adding the camera by Select Edit → Camera → Edit whilst that particular window is open and you will be able to double check all of the features demonstrated above Ensure that IP's, Usernames and Passwords are correct, as well as Camera privileges as all could be factors in why the camera is not connecting correctly. Failing this the camera may have a more physical network issue or an IP conflict could be present somewhere on the network.

4.1 Adding ONVIF Compatible cameras.

ONVIF is a global standard which is being adopted by a number of the main IP-based security products. ONVIF standardizes communication between IP-based products and the Azimuth Software. This allows us to provide a search tool to detect any ONVIF supported IP devices on your local network.

Edit > Camera > ONVIF Refresh brings up Azimuth's ONVIF discovery tool.

To start searching for ONVIF devices click on the button "Start Probe broadcasting". This sends a broadcast message to find any ONVIF supported on your local network. If ONVIF supported devices are detected they are listed in the "Serial Devices" box.



Device Probe

General

Discover new device on the network, and re-configure them. A broadcast message will be sent out and replies waited for.

Devices

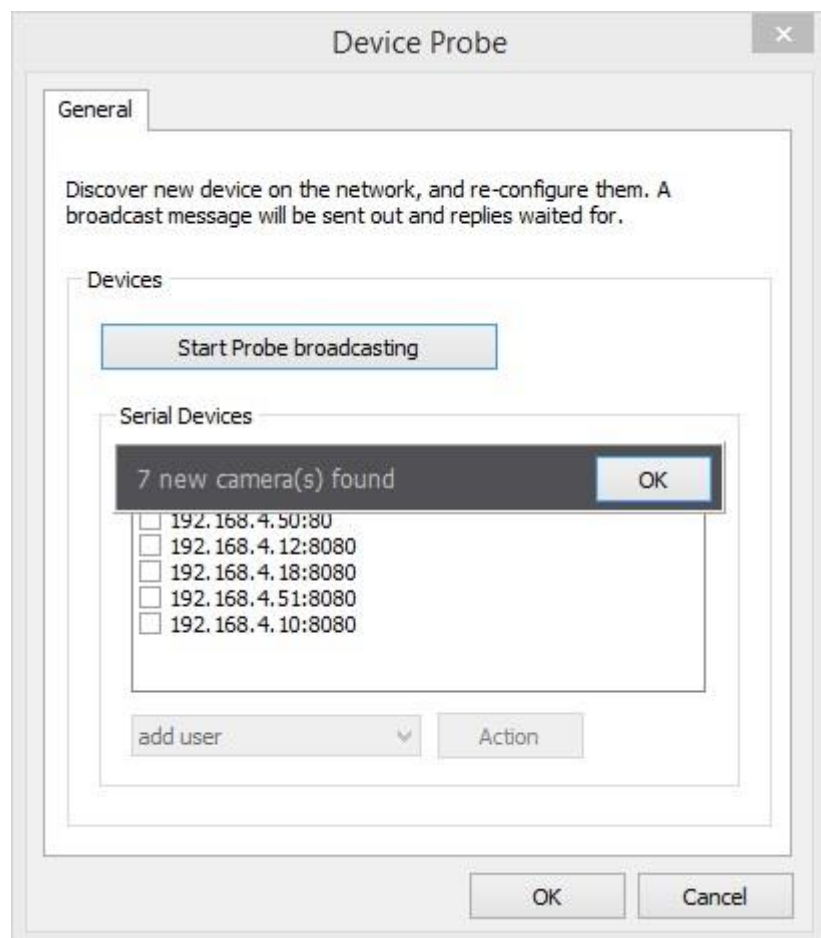
Start Probe broadcasting

Serial Devices

ONVIF searching...

add user Action

OK Cancel



Select the cameras which you want to add into Azimuth from the serial devices list. Azimuth will then ask you for the Username / Password for each of the cameras.

If the authorization is correct Azimuth will use ONVIF to retrieve all the configuration of the camera and it is then added within Azimuth.

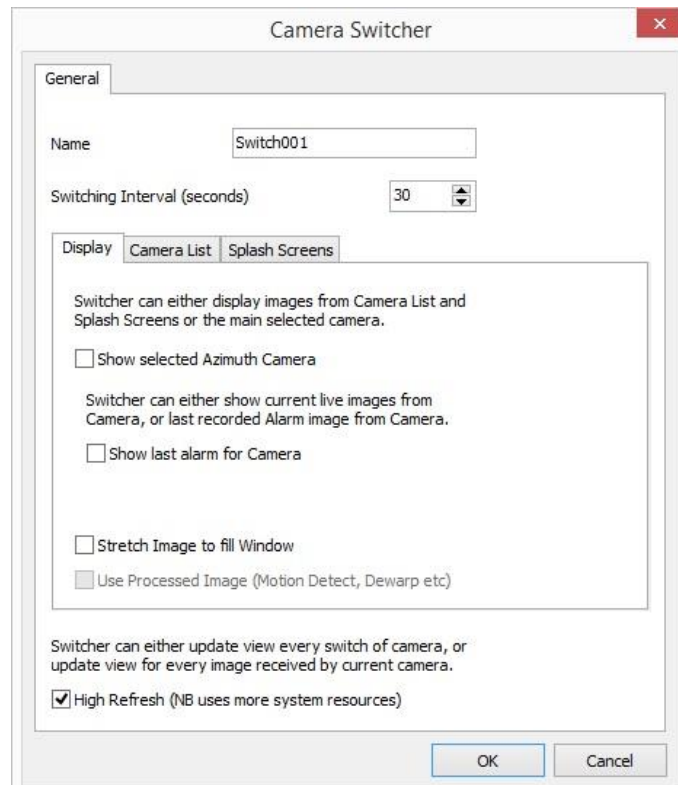


5.0 Camera Switchers.

Like its predecessor Azimuth allows the user to add a window that switches between cameras.

Details.

Head to Edit → Switch and a sidebar will appear. All of the options except for add will be grey-out if a Camera Switcher is not already applied. Click Add and the Switcher editing window will appear. At the top of the window you can name your Switcher and below that is a setting that allows you to determine how long each camera stays visible before changing to another.



Camera Switcher

General

Name: Switch001

Switching Interval (seconds): 30

Display | Camera List | Splash Screens

Switcher can either display images from Camera List and Splash Screens or the main selected camera.

☐ Show selected Azimuth Camera

Switcher can either show current live images from Camera, or last recorded Alarm image from Camera.

☐ Show last alarm for Camera

☐ Stretch Image to fill Window

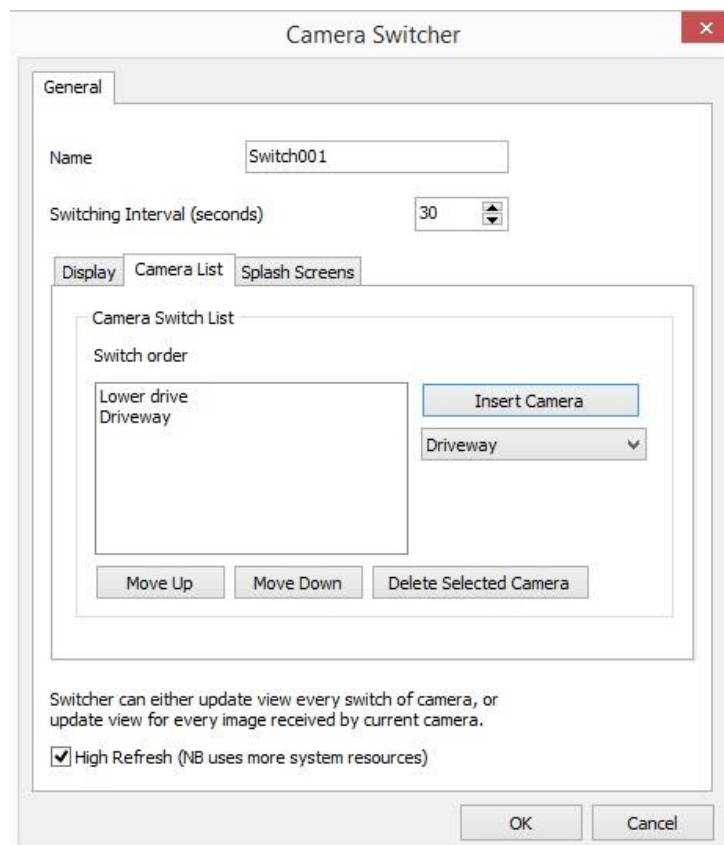
☐ Use Processed Image (Motion Detect, Dewarp etc)

Switcher can either update view every switch of camera, or update view for every image received by current camera.

☒ High Refresh (NB uses more system resources)

OK Cancel

Below this are 3 tabs. The first tab displayed asks you whether or not you would like current live images displays, or recorded images from the latest alarms. If ticking “Show Selected Azimuth Camera” the window will change, leaving two options at the bottom for stretching the image or using a processed image. If you have chosen to show live images from selected Cameras you must then chose which cameras in the following tab.



Camera Switcher

General | Camera List | Splash Screens

Name: Switch001

Switching Interval (seconds): 30

Camera Switch List

Switch order

Lower drive
Driveway

Insert Camera

Driveway

Move Up Move Down Delete Selected Camera

Switcher can either update view every switch of camera, or update view for every image received by current camera.

☒ High Refresh (NB uses more system resources)

OK Cancel

Here you will see a drop down box with a list of the systems cameras. Simply select each camera you require and click Insert Camera and it will appear in the list to the left. You can then either move up, down or delete any of the cameras by using the 3 buttons below.

The final tab allows for you to add a splasher screen, i.e a logo that will appear at the end of each cycle. Simply chose an image from your hard-drive by clicking on browse.

Once all this is completed, simply click OK and your new Switcher will appear.

6.0 The “Man-Machine Interface”.

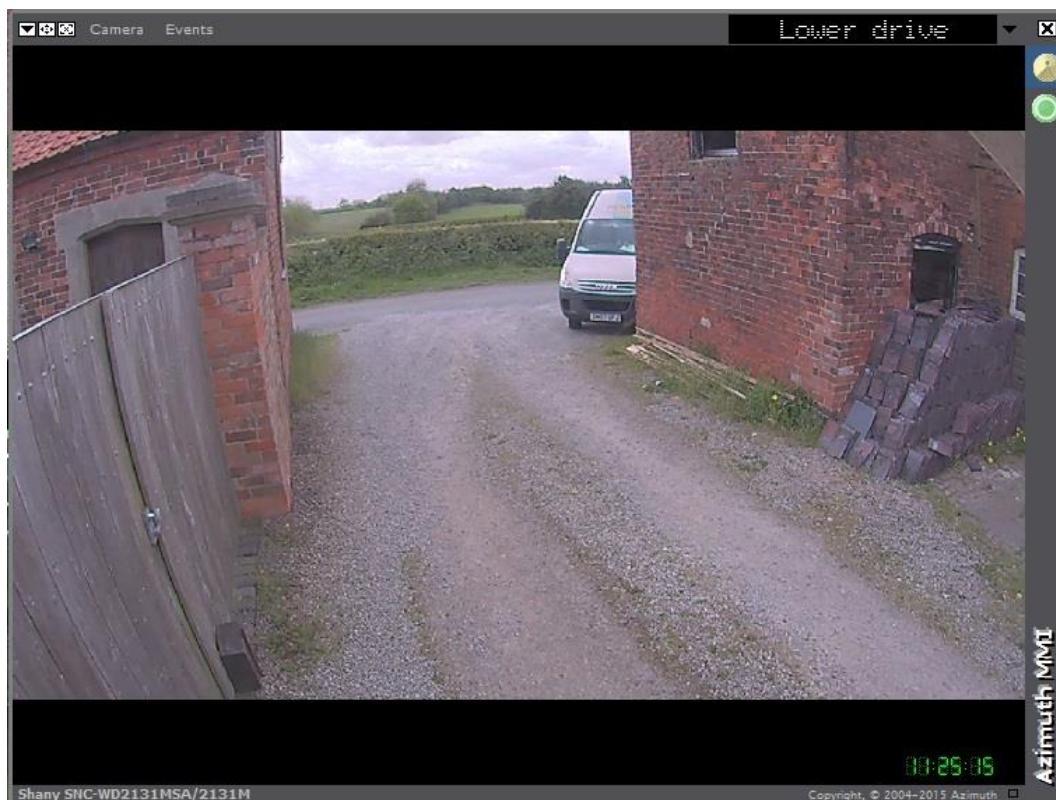
The “Man-Machine Interface” built into the Azimuth software is the gateway to many of the features on Azimuth and many of the individual settings for each of the cameras. It is also where an operator can source any recorded images and scan through footage recorded by the camera.

Details.

In order to open the Man-Machine Interface, simply highlight the camera required so that the window turns green, and click on the Azimuth logo in the top right hand corner of the window, as demonstrated below.



A new window will slowly fade into view. At the top you will see two options, Camera and Events. The Events tab is covered on page 45 of this manual. Under the Camera tab can be found the same details that were set when the camera was initially installed. Here you can change details for the individual camera such as IP addresses, user-names and passwords as well as frame rate and resolution settings. The two small icons in the top left corner are for the camera controls and a drop down box which enables you to start recording and how you'd like to record, as well as add or remove certain elements such as camera controls from the live view. If the Man-Machine interface PTZ (Pan Tilt Zoom) controls in the top right corner are shown as locked, simply head to View → Lock All Camera Controls which should be ticked and this will free up the PTZ Capability in the Live view. If the camera you are viewing is not a PTZ camera these controls will not show up at all.



The name of the Camera you are currently viewing can be seen along the top, with a small drop down box to its right. When dropped down it allows you to select a different camera without completely closing down the interface and having to highlight a new camera and start from scratch.

In the top right-hand corner can be seen two small icons, of which one should already be selected. If you hover over these two icons you will see that the one currently selected is for Live viewing, and you will at that point be looking at a live image stream from the camera. The 2nd Icon will take you through to any recorded images. Upon clicking this the window will increase in size and a date option will appear. You have three search options to choose from. The first is to select a day of the current week on the left hand side. If you are on Monday and you click Monday you will not get footage from the previous Monday. Once you have selected the day, click the Blue icon to the right. You can also click the green icon which will take you to the most recent recordings for that camera. The final Option is to click on the calendar on the right and select a specific date followed by clicking the Clock Icon to the right.



Upon selection of either one of the above three options the window will again increase in size until the section pictured below becomes visible. What you will at first notice is a time line with blue bars showing how much recording was captured and when. If this entire Bar is red it means that the camera has no recordings and you may wish to check your event settings. By hovering the mouse over each of the Icons and small tab will appear telling you what that Icons purpose is. By clicking on any one of the blue bars you should see an image appear in the window above, this is a sequence of images captured at the point from which the blue bar you select begins. For example on the image below by clicking in the longest blue bar, the first image will be at 14:00 as this is when that time section begins. By selecting the first Icon on the left hand side of the window you can chose to see only the Alarm images as opposed to a combination of alarm and timed images. The Purple Icon below that increases the size of the time bar allowing you to focus on much smaller time scale recordings. Below the time bar is a series of Icons that run from left to right:

Audio: If this is an enabled feature, you can select to have audio recordings turned on or off.

Play: This will play in real time the recordings from the bar you have selected. (You can increase the frame rate using the drop down box to its right).

Previous Block: This will take you back to the beginning of the previous 5 minute block.

Previous Frame: Will take you back to the previous image to the one you're currently viewing. This allows you to filter back frame by frame to find exactly what it is you're looking for.

Next Frame: Will take you to the next individual image, again allowing you to filter through each image one by one.

Next Block: Will take you to the next 5 minute block.

Add Current Image to Save List: This will add the image that is currently visible to the list of images/footage you wish to save.

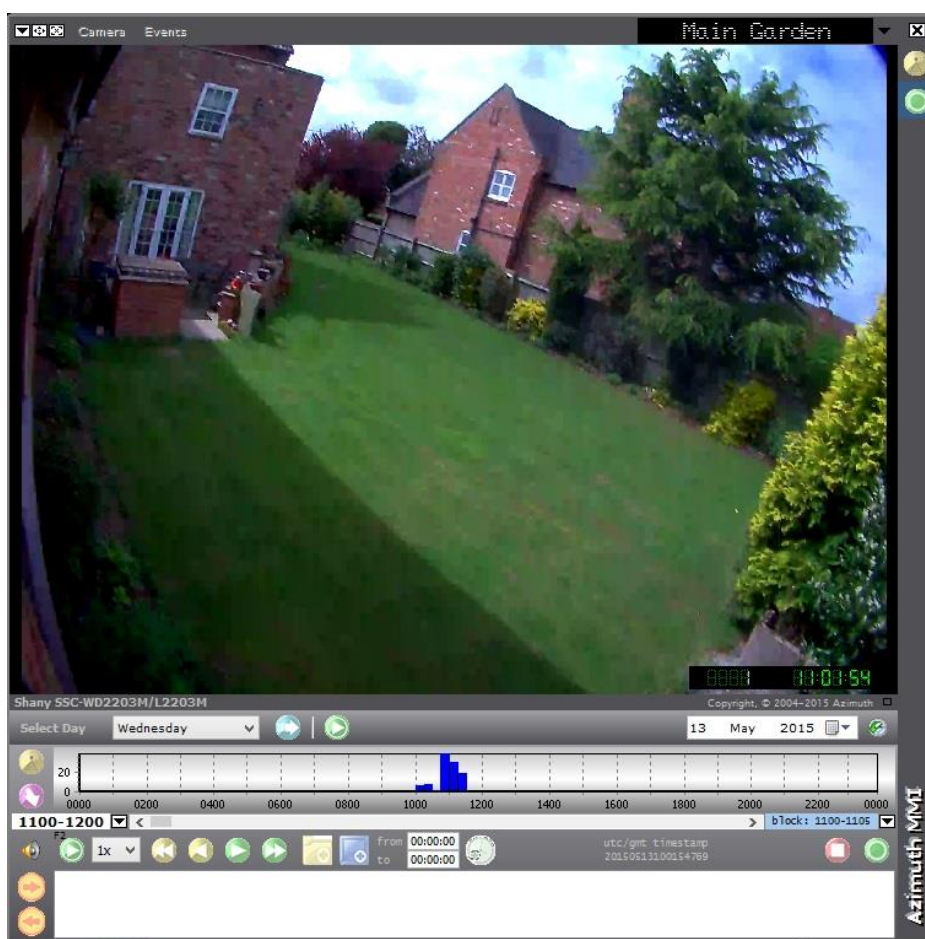
Add block to save list: This will add the entire block to the list of images/footage you wish to save.

Add time block to save list: To the left of this icon is an option to input a precise time. With this done you can click that time block icon and it will add those exact times to the list.

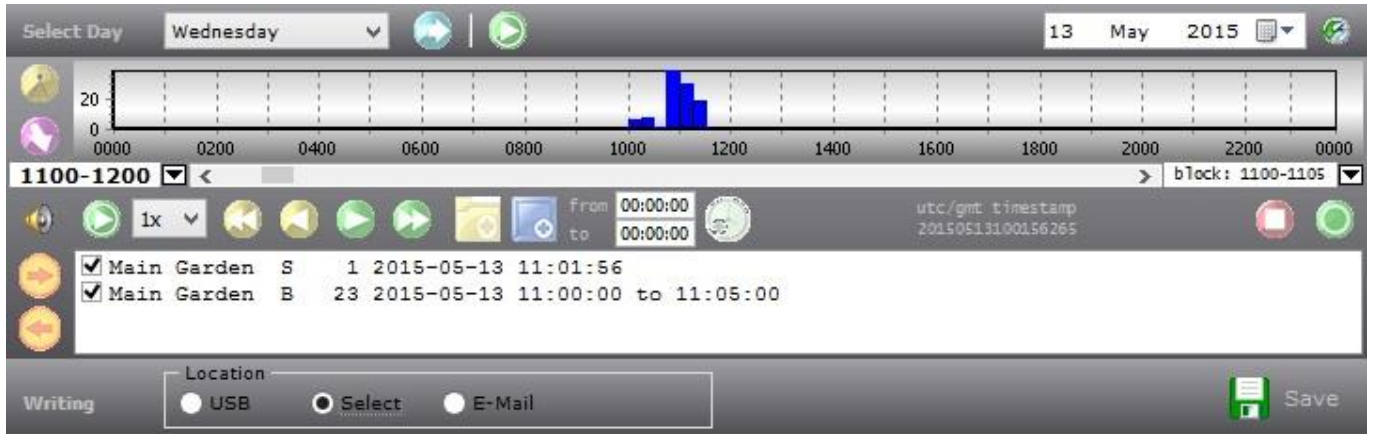
Delete Selected Files: Any files in the list below that are ticked will be deleted.

Save Selected files: Any files in the list below that are ticked will be saved.

To the right of the Save list are two more options, these are simply so that you can either select or unselect all of the items in the list.



Now that you have all the evidence in the save list, click on the green icon on the right and again the window will increase in size as shown below. Simply select how you would like the Items to be saved. By selecting "Select" this will allow you to choose a location with the PC you are using to save the footage.



Now click on “Start Save” after which another window will open. Here it will ask you which format you would like to the footage saved as and then you will be asked whether or not you wish for the footage to be saved into one folder or for the three different blocks to be saved to their own individual folders. At the following window you can select whether or not to have the time and date shown as a time-stamp on the image and where, and can also select the frame rate that the footage plays at. 1 per second means you will literally only see one frame per second. The more higher the frame rate, the faster it will play.

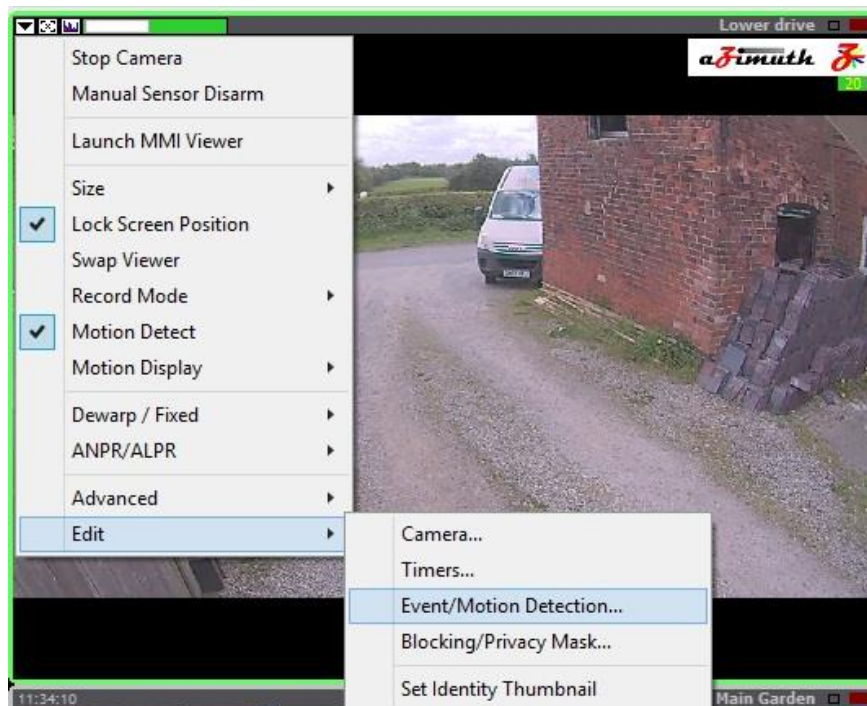
Now you will be asked where you want the footage to be saved followed by a progress bar as the footage is saved. Then it is complete, and you will be able to view your saved footage.

7.0 Motion Detection Settings.

Just like its predecessor Azimuth allows for cameras to be triggered via motion detection. By adding a net of cells to the image Azimuth looks for coloration changes to individual cells to sense movement. Sensitivity and other options can be altered to prevent changes in sunlight or shadows from creating false alarms.

Details.

You can gain access to the cameras event section in two ways. One is to go through the MMI by selecting “Events” at the top of the window. The other is to simply have the camera window highlighted (Green), select the drop down arrow in the top left hand corner and follow Edit → Event/Motion Detection. (as shown below)



Detection Method
☒ Inputs only
☐ MD Zone 1
☐ MD Zone 2
☐ MD Zone 3
☐ MD Zone 4

Method Events
☐ Motion Detection
☐ ANPR / ALPR
☐ Track and Zoom

Cells (Key)

On (This zone)

On (Other zone)

Off

Event/Motion Detection

Summary
Patrols
VerifiedAlarms
Motion Detect
Track and Zoom
ANPR / ALPR
General

All configuration for Detection Methods

	MD	Cells ON	Min	Max	Sensitivity	T and Z	ANPR / ALPR
Inputs only	off	0	-	-	medium medium	off	off
Track and Zoom : <none>							
MD Zone 1	on	375	5	281	very low low	off	off
Track and Zoom : <none>							
MD Zone 2	on	0	-	-	medium medium	off	off
Track and Zoom : <none>							
MD Zone 3	on	0	-	-	medium medium	off	off
Track and Zoom : <none>							
MD Zone 4	on	0	-	-	medium medium	off	off
Track and Zoom : <none>							

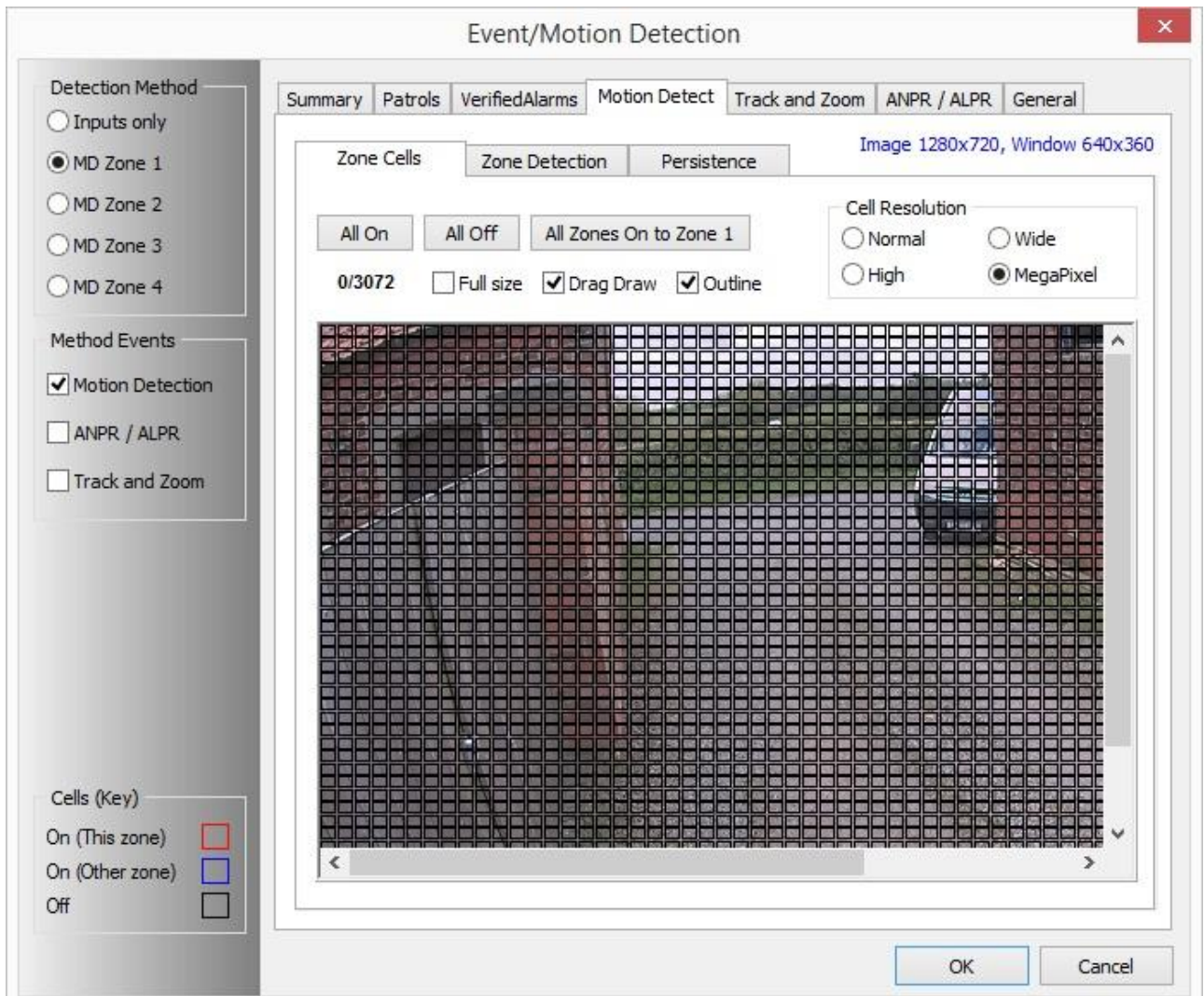
Set all Zones to Defaults
375 cells ON out of total of 3072 available

OK

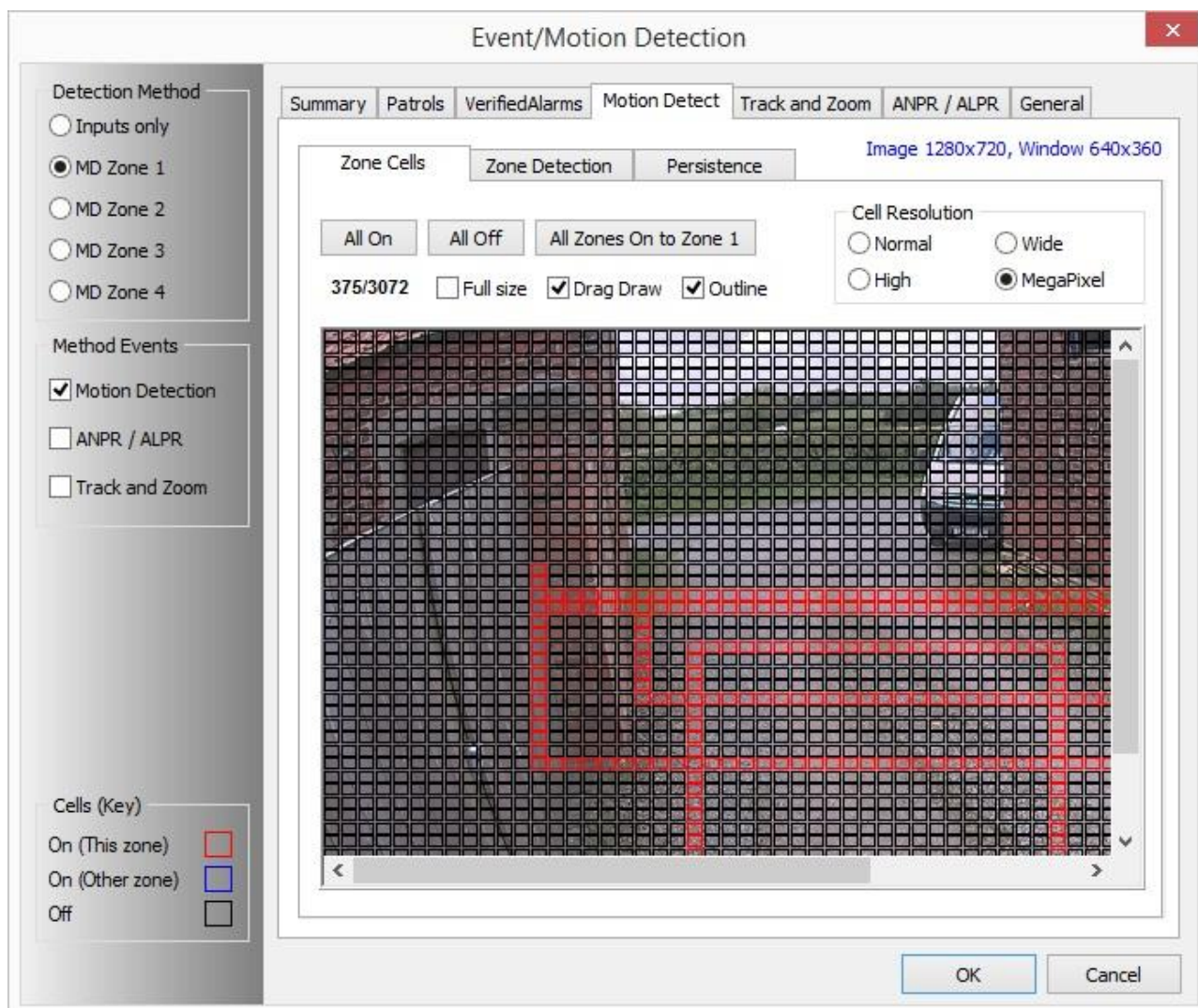
Cancel

Upon selecting either of these options you will be faced with the window above. The first tab you will see is the Summary tab and this will just give a series of details relating to settings that are already in place. Note that down the left hand side you see a list of selectable options. As default the window will open on the Digital section, this section will be covered in another section of the Manual. You have 4 different Zones available, and each have the same settings available to change for 4 different zones of Motion Detection to one camera. This is so that a user can set 4 different area if each if these areas requires different settings.

Select Zone 1 along the right hand side and select the "Motion Detection" tab.



Initially “Normal” Cell sizes will be present, and they should all be red. When they are red it means they are set, so first select “All Off” and they should all turn black giving you a blank Canvas. In order to turn a cell on simply click on it, or alternatively drag a square or rectangle to set a cell window. Setting Cell windows is important, as making a solid block of active cells will make it difficult or impossible to prevent false alarms, whereas cell windows work just as well as in order for a target to move across an image it must pass through at least one side of the window activating cells. You can change the detailing of the cell resolution on the right hand side. Normal being the standard, with the other being more defined. This should all depend on how detailed you wish for you motion detection to be.



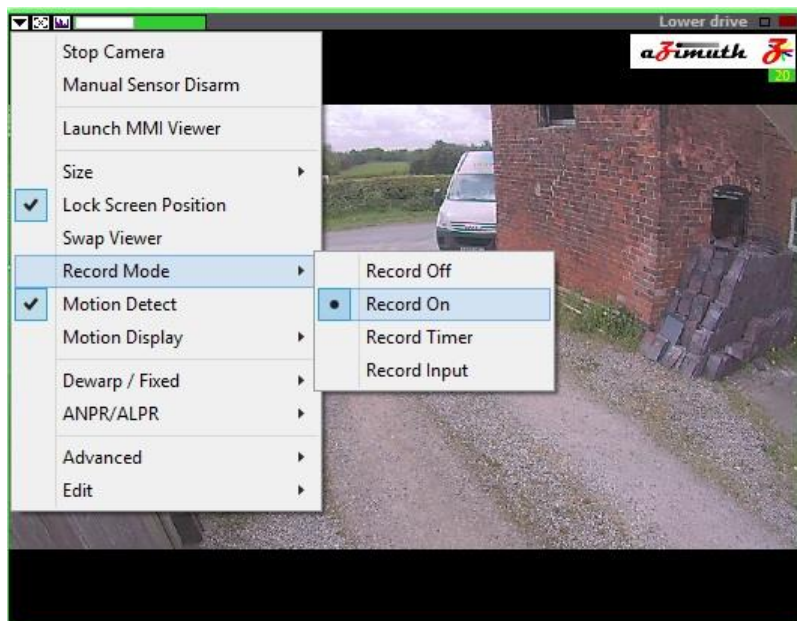
As can be seen in the above image, a series of Cell Windows have been set up to cover the road and pavements. By putting in these windows anyone entering must pass through at least one, but by not making solid blocks of active squares they won't be setting off excessive cells. Why this is important is explained below.

By selecting the “Zone Detection” tab you are taken to a section that deals with sensitivity and the prevention of false recordings. Obviously one thing that a camera can't do is tell the difference between a human and Wildlife such as badgers or foxes. Much of an external cameras false recordings are of wildlife wondering in front of cameras but this can be prevented using the settings in this section. The green bar in the middle of the screen is sensitivity, during the day sensitivity need only be set low, but using the “Night Mode” tab sensitivity can be set to a different level by night.

Below that is the cell limiter. This part is how you will eliminate false alarms by anything smaller than a human, or larger (Such as shadowing or changes in sunlight) setting off the recording. By increasing the number of cells in the first box you are setting it so that anything triggering any number of cells BELOW that number won't create an alarm, and anything triggering more than in the second box will also not create an alarm. You can use the 4 options below to set it to a pre-defined level. What this means is that something like a Badger or Fox triggering 4 cells when the range is set from 5 will be ignored, and if they range is 5 – 120 cells but a change in sunlight triggers all of the cells, it will again be ignored. This will need to be tested to ensure that anything smaller than a human will be ignored, and anything larger than a car will also be ignored, but of course it is entirely down to user preference.

The final tab in the Motion Detection section is “Persistence” this is how many times a cell needs to be trigger before it begins to record. If you wish for Azimuth to be sure something is moving within that cell, set the number higher so that the cell has to be activated more than once for recording to begin.

Once all these settings are in, Click OK at the bottom of the window and set up for Motion detection is complete. Now all you need to do is ensure the camera is set to use Motion Detection when recording.



To do this highlight your camera window, and select the drop down box. Ensure “Motion Detection” is ticked, and that recording is on. Once this is done a small box in the top right hand corner of the camera window will turn to a dark red, and this will turn to a brighter red when recording is in progress. As default the camera window will show which cells are being activated (they will appear on the screen when Active) and in order to turn them off you will have to re-open the event window and head to the very last tab “General”. In there you will have to un-tick the option “Display motion cell indicators in Viewer” and the cells will no longer show up when activated in the Camera Viewer.

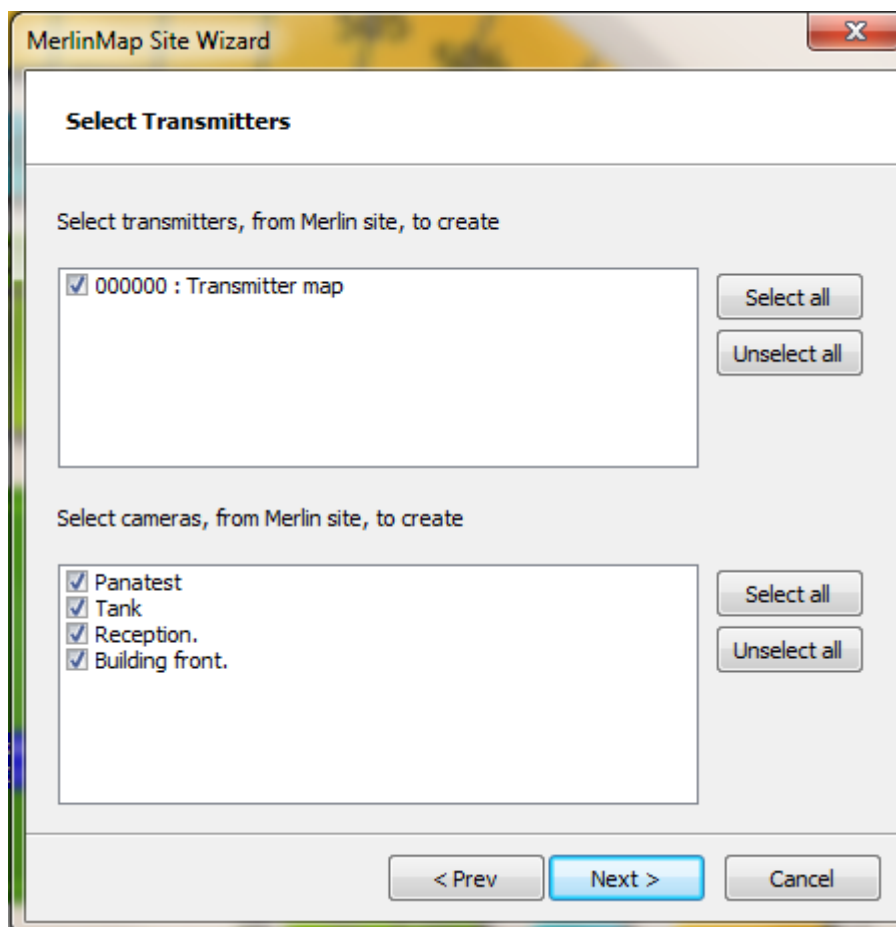
8.0 Mapping.

Each Azimuth server can have a map of camera locations added to the system for use on a dual screen. This allows an operator to see in real time the precise location of a camera activation at any one time. Used correctly, the program is most likely to be used functionally during a locations none operational hours when a camera activation can be deemed a legitimate security threat. Setting up the system is as follows:

Following the menu options **Edit → Site Map** will open up the mad editor in a separate window, and will initially be blank. If this flags an error message stating that an image file is incorrect of that it has an invalid floating point then simply continue through by clicking “OK” and it will allow the editor to open.

If faced with a blank page, right click on the main screen and select Edit. In this window it is necessary to select a file path to the image you wish to use as your main map. You do this by again clicking edit and locating your required image file. Please note that character length on the file location cannot currently exceed 100 characters, so first ensure that the total number of characters in that image file path does not exceed that maximum. If it happens to exceed that maximum, then the mapping editor will simply ignore the path and return to a blank screen. Once you have selected your file path and it is correct click “OK” and your main image will change.

From having setup your base map, you now need to add your site and your icons and position them relative to where they are located on a property. To do this, simply right click and follow **New Plan -> Create Site**. Under the first option select Next, and then you will see the following frame.



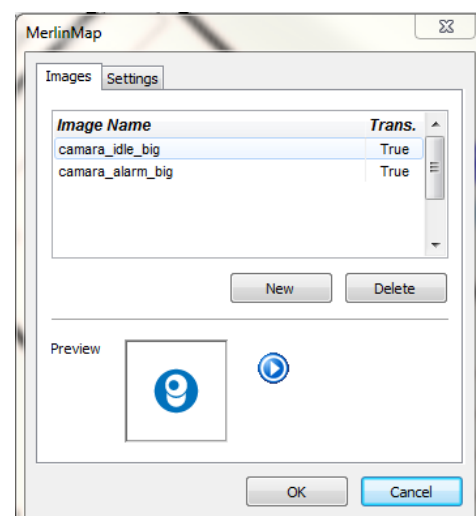
Here you will select your transmitter. Since you are doing this through Azimuth there will only be one transmitter available, as this map will need setting up per server. Below you will see your list of cameras, allowing you to select or deselect whichever cameras you wish to have on your map. The final two sections are not important as the application will automatically and evenly distribute your icons across the image ready for you to click and drag to the necessary locations on the image.

Once this is complete ensure that every time you have made a change that you head to **View→ Save Settings**. It may be necessary to restart the application on occasion if items do not automatically change.

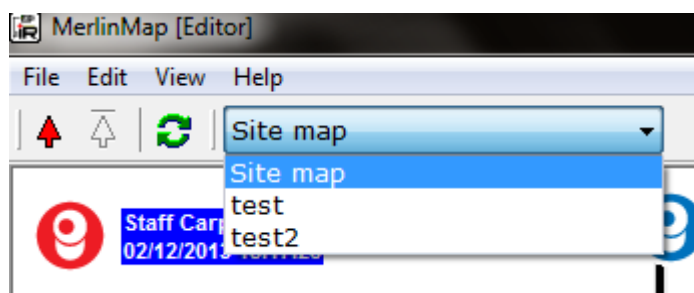
Initially all icons will appear as question marks within a green circle, as this is the generic Icon and will need changing. The process to do so involves adding either static or animated GIFs to the database, with the latter usually used when a camera goes into alarm. To do so, select **Edit → Images** and here you will see a list of Icons already installed. If none exist in the database it will appear empty. To add a new one, simply select "New" and find the file location on your system. Animated icons can be checked by clicking the small icon next to the preview.

You then need to right click on an icon (camera) and select Edit. A new window will be appear showing all details about that particular channel. You will also notice this allows you where to position that flag that sits next to the Icon to show what channel it is, it can even be turned off. Following this, select **View** and **Feature States**. All other sections can be disregarded, as the system automatically populates most sections.

Under Feature States you will see the cameras do different states listed as Camera and Camera Alarm. Under Camera you will select the icon you wish to appear when the camera is not under an alarm condition, whereas under Camera Alarm you will choose an icon that you wish to use in an alarm situation (most likely an animated GIF). You simply choose each one from the drop-down box of available icons at the bottom right of the window. Once complete, click OK and OK again. You will notice your icon change. Repeat the step until each Icon has been changed.



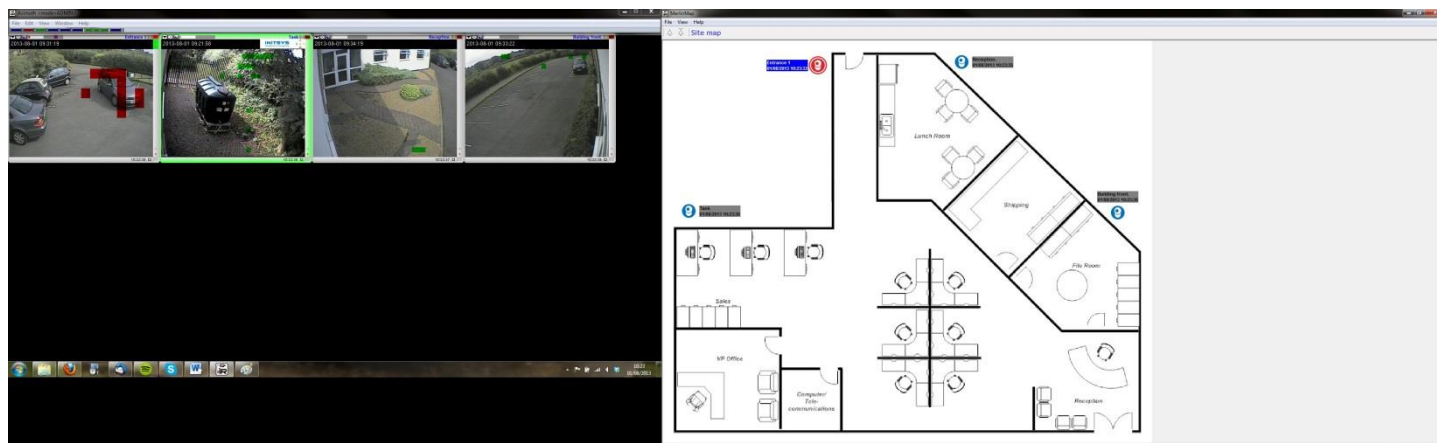
It is then possible to add an infinite amount of layers that can be selected from a drop down box at the top of the screen. The purpose of the layers is to represent multiple floors or areas of a property allowing you to be more detailed in the placement of your icons.



To do this, right click and follow **Layers → New**. Firstly it will ask you to select cameras, but if you have already selected the use of that particular servers cameras this window will remain blank to prevent the duplication of camera Icons within the Map. Following this it will ask you to select transmitters, and in the case of Azimuth Map it refers to iDigital or PIOS input devices and their channels which can also be added as Icons to a map layer. You can select or de-select as many of these as you wish.

It will then ask you for an image file, and the same rules apply as with adding your base layer in that there will be a 100 Character limit. Finally it will ask you to name the layer as it will appear in the drop-down box of layers, and the process is complete. Each icon can then be moved to a different layer, but right clicking, selecting Set Layer, and choosing the layer you wish for that Icon to sit on. The final process is then to position your icons to the correct locations.

With the system set up correctly, any cameras going into a record mode will show up as flashing Icons on the map.



As demonstrated, the “Entrance 1” camera has gone into alarm, recording a vehicle entering the premises, and the mapping software has gone into alarm to demonstrate exactly where this camera is located.

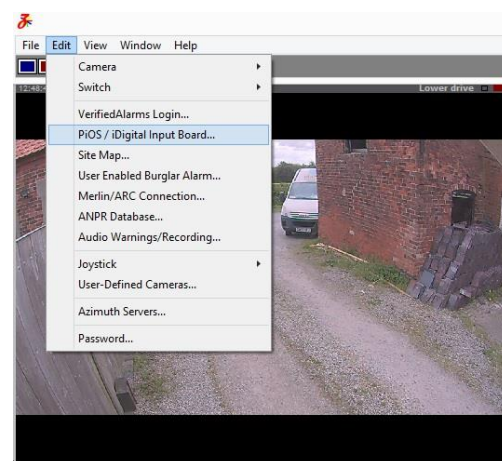
9.0 iDigital Setup.

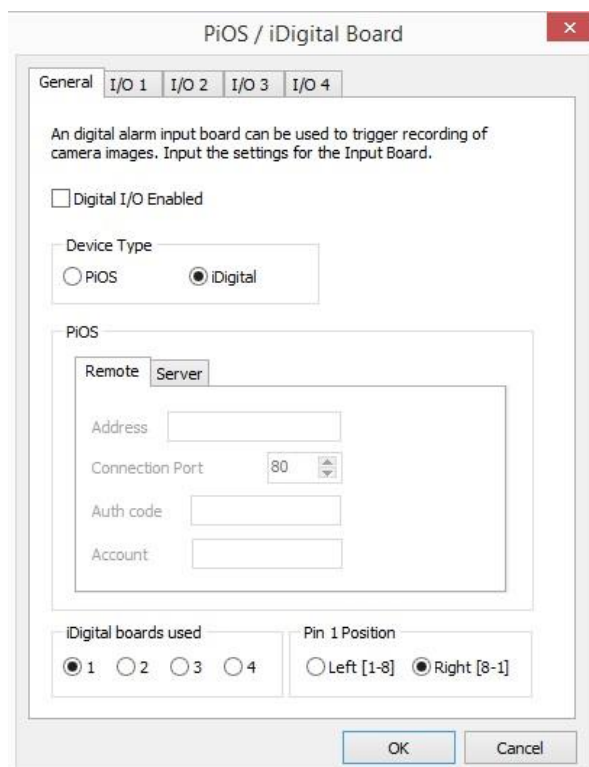
An Idigital device can be used to trigger cameras using PIR's as opposed to Motion Detection. In some outdoor environments Motion Detection might not be suitable whereas a PIR may be a much better solution. They can also be used to make camera jump to pre-assigned presets when a certain PIR is triggered, allowing a camera to follow a target.

Details.

Each Idigital board has 8 inputs, and 4 can be added to Azimuth at any one time. The Idigitals need to have an IP assigned to them using a special software called Hercules. Once this is set up they can be added to Azimuth.

To add an Idigital, head to Edit → Idigital Input Board.





PiOS / iDigital Board

General I/O 1 I/O 2 I/O 3 I/O 4

An digital alarm input board can be used to trigger recording of camera images. Input the settings for the Input Board.

☐ Digital I/O Enabled

Device Type
☐ PIOS ☒ iDigital

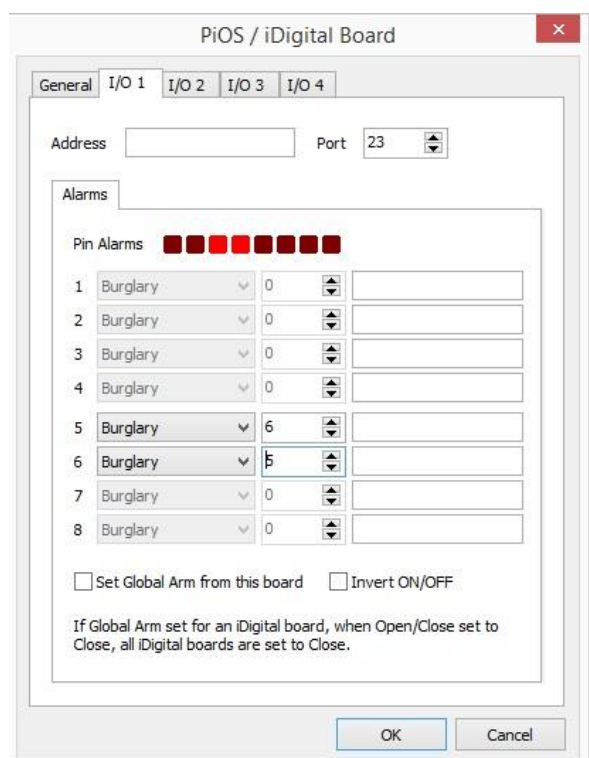
PIOS
 Remote Server
 Address
 Connection Port 80
 Auth code
 Account

iDigital boards used
☒ 1 ☐ 2 ☐ 3 ☐ 4

Pin 1 Position
☐ Left [1-8] ☒ Right [8-1]

OK Cancel

The window on the left will appear. In the first tab simply select how many iDigitals you will be using (Azimuth needs this information for the Signal LED's explained below) and tick the box to Enable the iDigitals. Head to the first iDigital Tab.



PiOS / iDigital Board

General I/O 1 I/O 2 I/O 3 I/O 4

Address Port 23

Alarms

Pin Alarms ■ ■ ■ ■ ■ ■ ■ ■

1	Burglary	0	
2	Burglary	0	
3	Burglary	0	
4	Burglary	0	
5	Burglary	6	
6	Burglary	5	
7	Burglary	0	
8	Burglary	0	

☐ Set Global Arm from this board ☐ Invert ON/OFF

If Global Arm set for an iDigital board, when Open/Close set to Close, all iDigital boards are set to Close.

OK Cancel

In this section, add the IP address and Port number. The section below is only relevant when you wish to send alarms to Merlin3. By Selecting which pins are active, what they are, and what their channel number is, the iDigital can send alarms to Merlin. But to assign them to the triggering of cameras you will need to go back to the events section. Once your iDigital boards are added you can turn on the iDigital Status LED's, that show when an Idigital is live and when it is being triggered, but following File → Show iDigital Status.

In doing so a series of LED's will appear along the right hand side.



Each of the larger Green LED's signifies a live iDigital, with the lower level of LED's showing when an Output is triggered and the upper level of Red LED's showing when an Input is triggered. Using these LED's it is easier for walk tests to be conducted to ensure an iDigital is being correctly triggered by a PIR. Further settings follow.

In order to use an iDigital for recording or sending a camera to Pre-sets, re-open your events section for the relevant camera, leave "iDigital" ticked on the left hand side, and select the Patrols Tab.

Detection Method
☒ Inputs only
☐ MD Zone 1
☐ MD Zone 2
☐ MD Zone 3
☐ MD Zone 4

Method Events
☐ Motion Detection
☐ ANPR / ALPR
☐ Track and Zoom

Cells (Key)

On (This zone)

On (Other zone)

Off

Event/Motion Detection

Summary
Patrols
VerifiedAlarms
Motion Detect
Track and Zoom
ANPR / ALPR
General

Camera can patrol between Memory / Preset positions or automatically return to a Preset after a timeout period.

Normal / Day Mode
Night Mode
Inputs

Camera can patrol to Memory / Preset position on iDigital / PiOS Pin being active.

I/O 1
I/O 2
I/O 3
I/O 4

1
Home

2
Home

3
-- position --

4
-- position --

5
-- position --

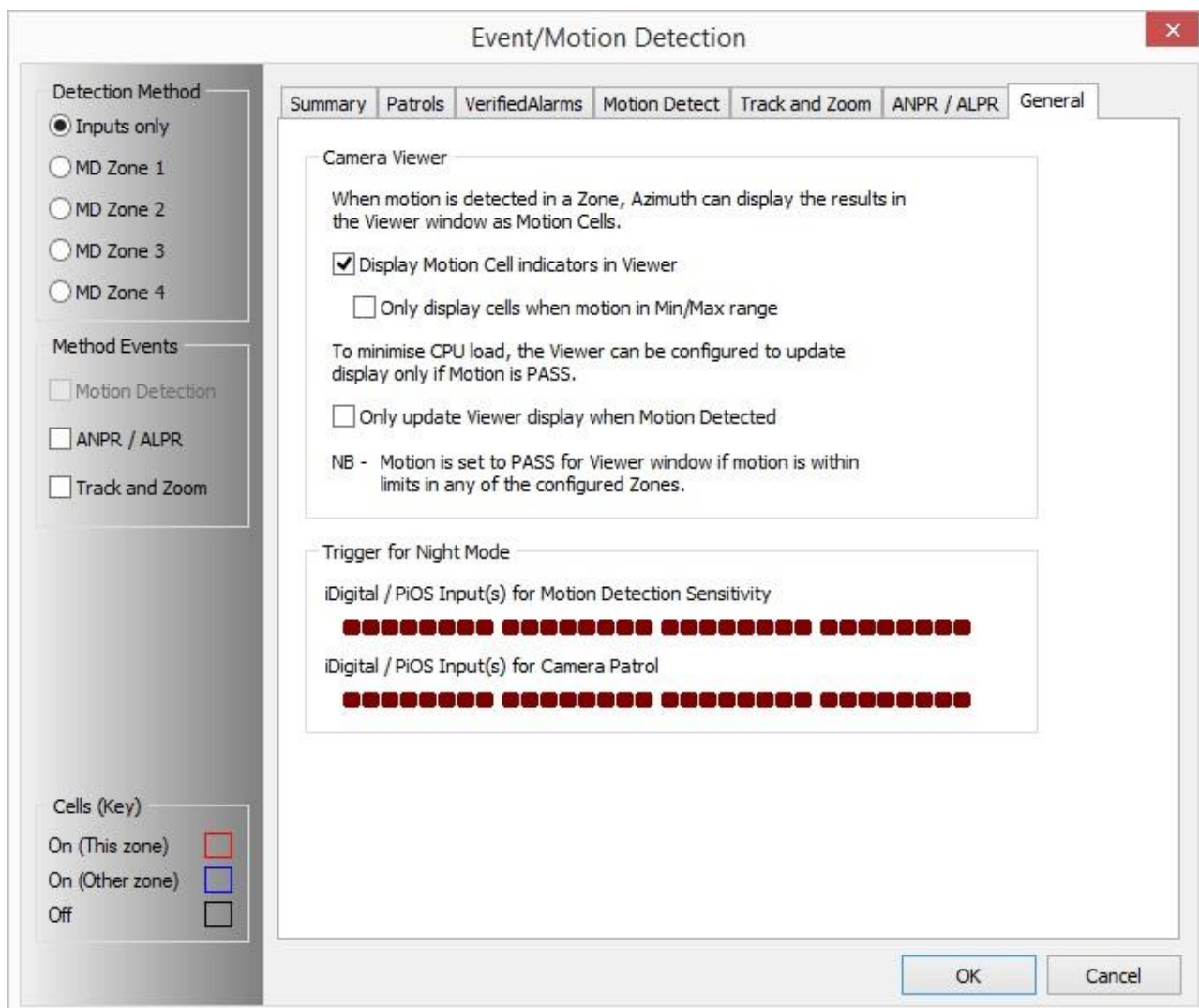
6
-- position --

7
-- position --

8
-- position --

OK
Cancel

By selecting the "Idigital Input" tab you will be faced with another 4 tabs showing each of the boards. Under each of those is list of drop down boxes and you simply need to select which presets you wish each of the inputs to trigger. This means, for example, when Input 1 on the Idigital triggers it will send a command to the camera for it to return to its Home position. What this allows is for a perimeter fence to have a chain of PIR's installed along its length that can trigger the iDigital and in turn send a command to the camera to move to a pre-set looking at the area that particular PIR is covering, allowing a camera to follow a target.



By heading to the General tab you can also select which inputs on the iDigital board you wish to use to simply trigger the recording of that camera, as shown above. If you wish for the iDigital to move a camera to its Pre-sets and record whilst doing so, ensure that both of these sections are set.

10.0 Setting up Patrols.

Some cameras can patrol between Memory/Presets positions or automatically return to a preset position after a timeout period.

In order for this feature to work you must be using a camera that is PTZ and also allows for Pre-sets positions to be added in its own software.

Details.

Before programming the Azimuth side of patrolling you must add the presets into the cameras own web browser software. If after setting these Pre-sets they do not work within Azimuth it is recommended that checks be made with Azimuth LTD direct to ensure that the particular camera you are programming to work with Azimuth is fully compatible. In order for this section to work Azimuth has to send controls to the camera direct, in order for it to move.

×

Detection Method

☒ Inputs only

☐ MD Zone 1

☐ MD Zone 2

☐ MD Zone 3

☐ MD Zone 4

Method Events

☐ Motion Detection

☐ ANPR / ALPR

☐ Track and Zoom

Cells (Key)

On (This zone)

On (Other zone)

Off

Event/Motion Detection

Summary
Patrols
VerifiedAlarms
Motion Detect
Track and Zoom
ANPR / ALPR
General

Camera can patrol between Memory / Preset positions or automatically return to a Preset after a timeout period.

Normal / Day Mode
Night Mode
Inputs

Type

☐ None
 ☒ Patrol
 ☐ Return

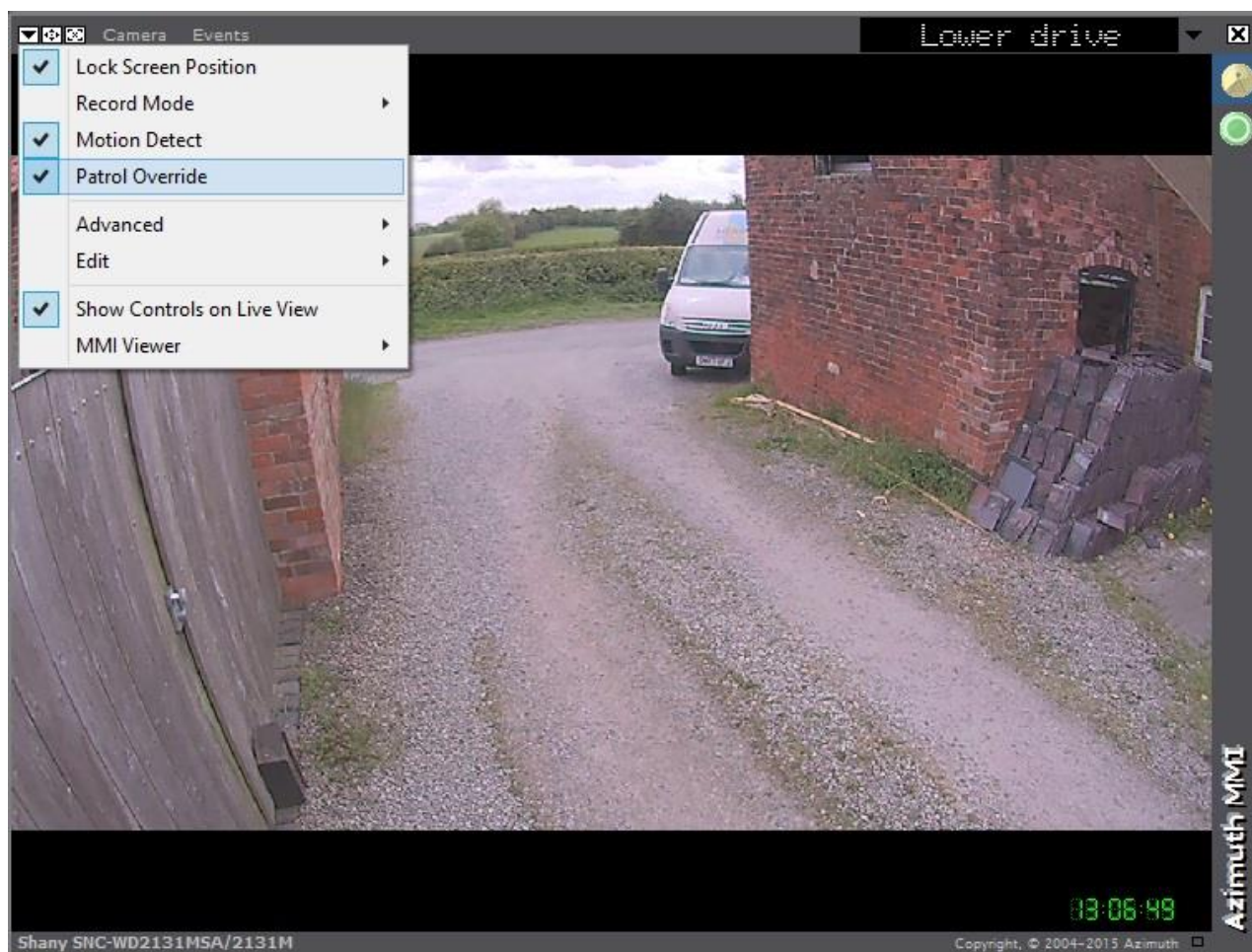
Memory / Preset Positions

Cycle / Return period (secs.) 10

OK
Cancel

The image above shows how in the events section, under patrols a series of Blue LED's can be selected that represent the pre-sets in the camera. Above this you have three different types of Patrol. None, which turns patrols off, Patrol, which will send the camera commands to patrol through pre-sets on a cycle, and Return which will automatically return the camera to an individual pre-set if the PTZ has been moved by an operator. If Patrol is selected, simply highlight the pre-sets you wish to use (By hovering the mouse over each one, it shows which number pre-set it is) and then below select the amount of time you wish for the camera to remain on each Pre-set. If return is selected you simply have to select which pre-set you wish the camera to return to, and how long you wish for Azimuth to wait before it returns the camera to this position.

If an incident takes place whereby the operator needs to be able to view an event as it happens without the camera moving on its patrols, it can be over-riden with the click of a button without having to completely remove all settings to stop the camera from moving. Open up the MMI for that camera and head for the drop down arrow in the top left hand corner. In this section there is an option for Patrol Override and ticking this will disable the patrol. It is important however that it gets turned back on once the Override is no longer required.

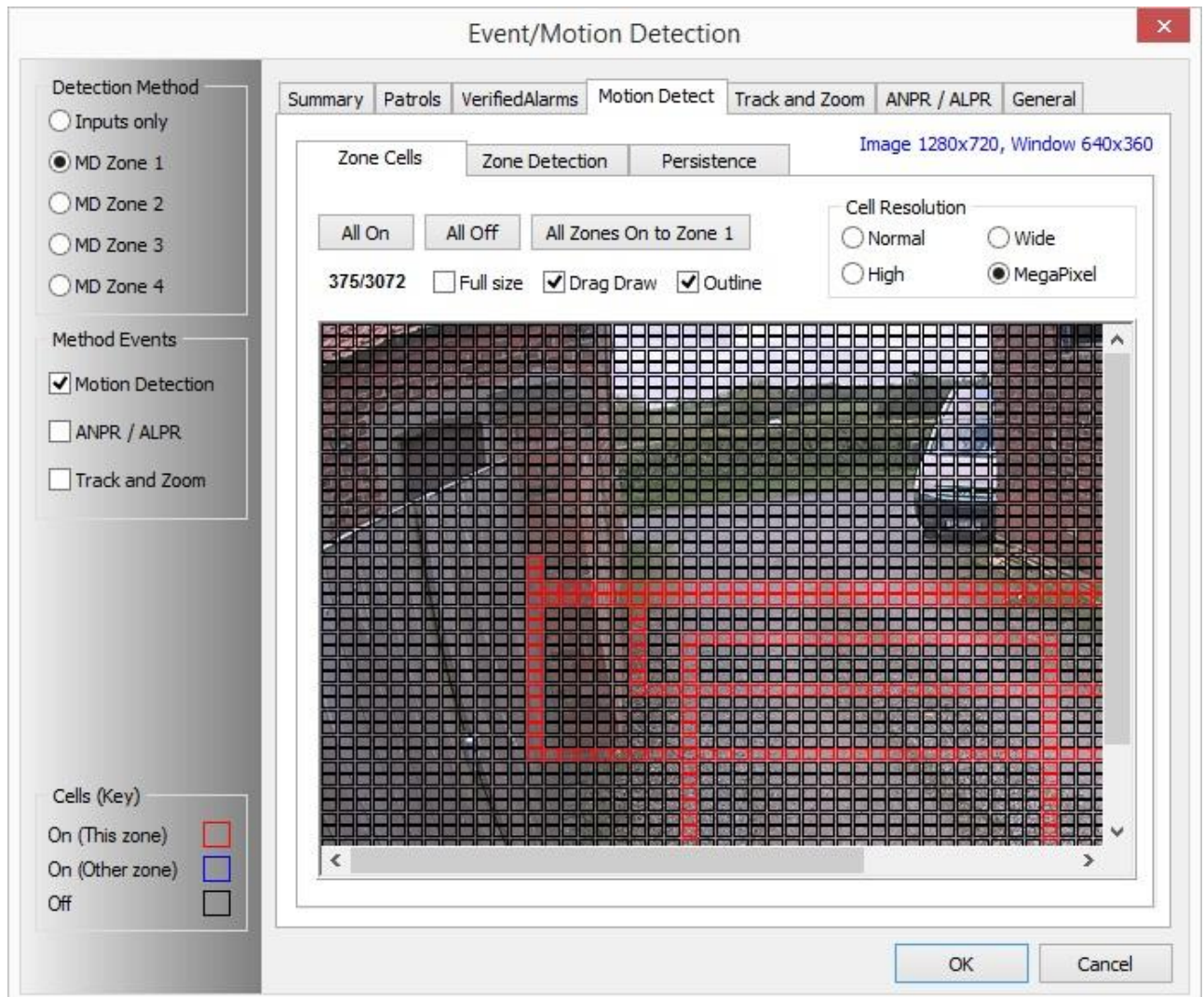


11.0 Track and Zoom.

Using track and Zoom it is possible to use one camera to trigger another. What this does it allows one camera to look for movement in a certain area and tell another camera to look at it in more detail.

Details.

First you need to choose a “Master” camera, this is the camera that will be used to trigger another camera into life. If the below example is used, it can be seen monitoring the entrance to a court yard. Although showing a good overview of the yard it may not be good enough to see a vehicles number plate for example, or capture an intruder’s face, but it could be used when Motion is detected to put another camera into recording.



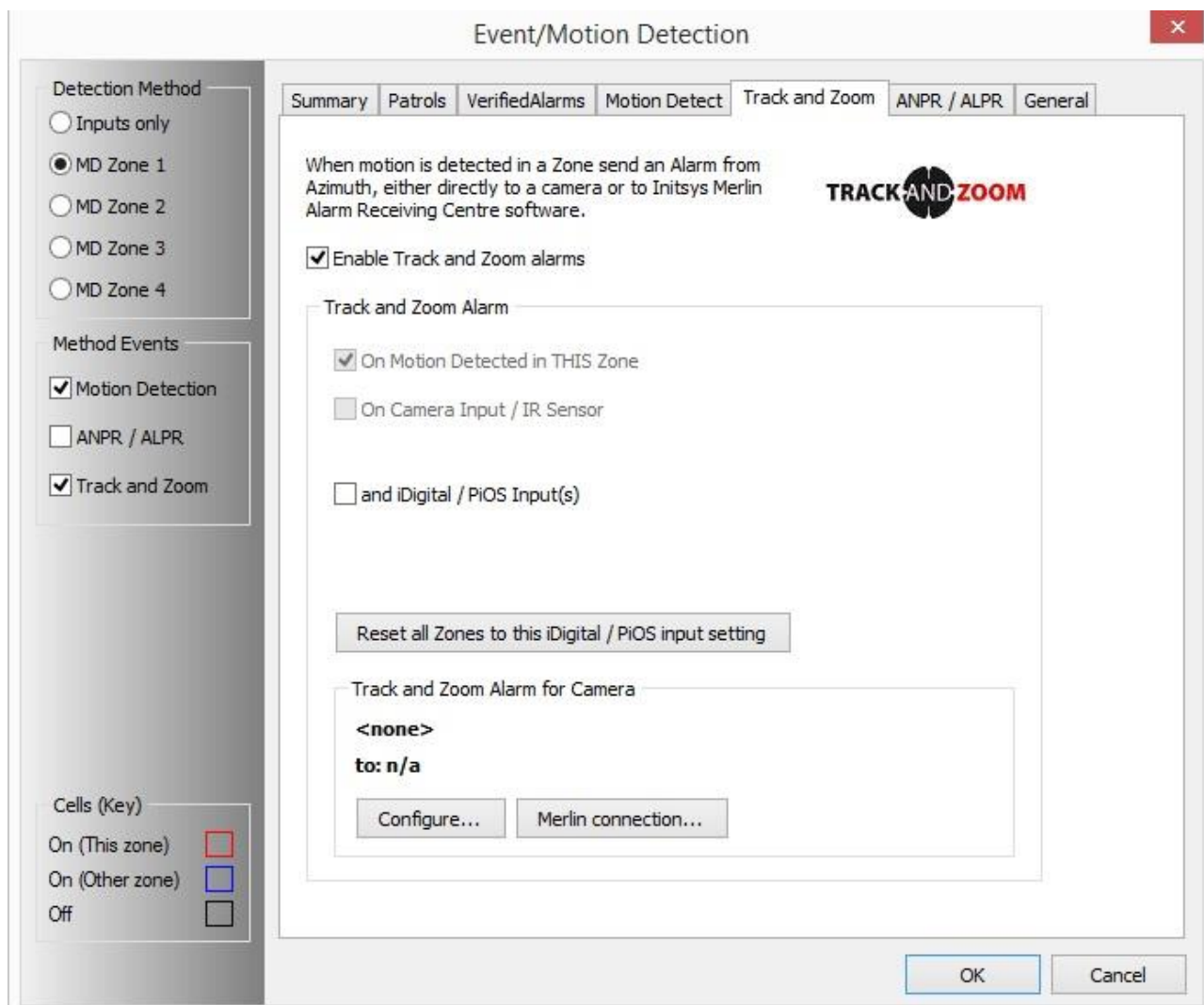
Check the enable Track and Zoom alarms.

These settings are independent to this zone, more zones can be configured using the same master camera.

If you are using motion detection and/or iDigital inputs then check the box and highlight the input you are using.

Once you have selected the method input you require for that zone, configure the remote camera that will Track and Zoom.

In the above example a court yard entrance is being monitored by the "Master" camera. If you wish for it to trigger another camera you must first select "Track and Zoom" on the left hand side and it will automatically take you to the correct tab.



Enable track and Zoom alarms. (This should be ticked by default) and then head towards the bottom where you will see “Configure” and “Merlin Connection”.

Click Configure and select either Local or Remote. If it's local it means it is from the same machine, whereas remote means it is from a different machine in a different location. The advantages of being able to assign a camera from a different machine is if you're monitoring a large site with more than one building and more than one system. If you have selected Local, simply follow the steps to assign the new camera. If selected Remote it will ask you for the same details that will have been input when a Camera was initially added.

12.0 VSaaS Setup.

The Azimuth software can be set up to send images to the Azimuth FTP service, Verified Alarms. One of the key advantages to this is that it enables cameras that don't have their own FTP details to send images to Verified Alarms as Azimuth acts as the sender.

Details.

The main access parameters for VerifiedAlarms are setup through the main menu > edit > VerifiedAlarms Login

This will open the window below. Input the details on the initial page. You must have already created a Verified Alarms account and added the cameras that you wish to be sent. The Username and Password it asks for are not your Login details to Verified Alarms, they can be found on your Print Tech Document that lists all of the camera File Paths. Ensure that these details are correct. The host address can also be found on this document and will usually be uki01.verifiedalarms.co.uk. If you wish for alarms to begin sending instantly ensure that Alarm sending is active is ticked. You can conduct a test to check that Azimuth is able to connect to the FTP Server.



VerifiedAlarms Login

General

VerifiedAlarms can be used to receive alarm images triggered by Azimuth. Input your login details for VerifiedAlarms.

☒ Alarm sending is Active

Login Latency iView

Login Settings

Username Ben

Password Edit... ..

Host address gs01.vsaas.com

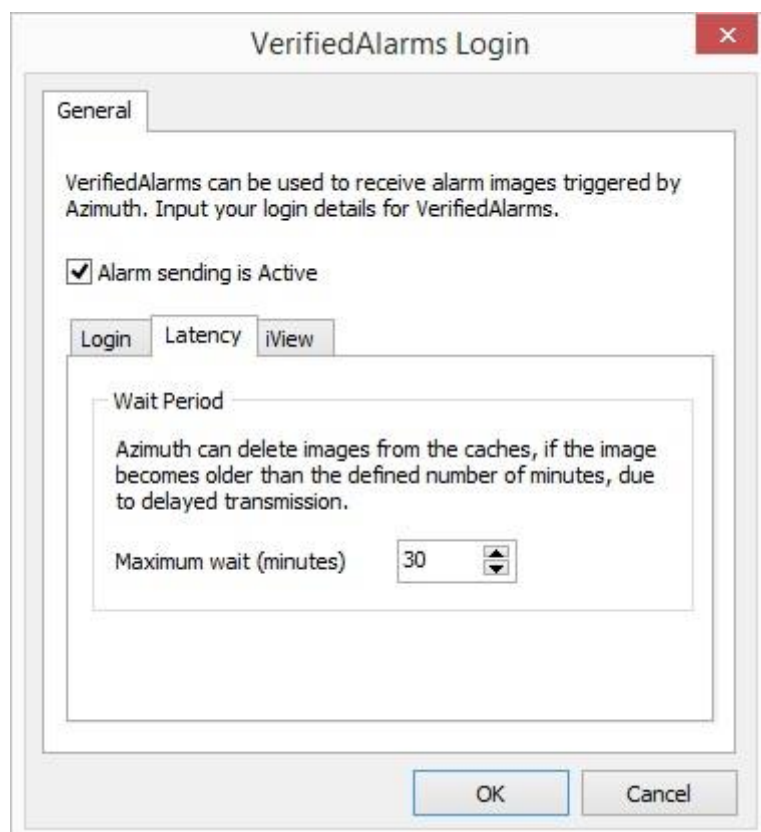
Start Test Stop Test ...

OK Cancel

Part of the way Azimuth works when sending images to an FTP server is to send Cached images so that there can be pre and post alarm images. If you select the latency tab you can define how long Azimuth will keep hold of cached images. Beyond this time the images will be removed from the cache.

The final tab in this window is iView, which allows for images to be stored to a folder in any FTP. Insert the correct file path, and any images recorded pre-post alarm will be sent to this folder for viewing as JPEGs.

You must now add the path to the individual camera so that it can send it Verified Alarms. Highlight the desired camera and using the drop down arrow follow Edit → Camera and select the alarm tab. Here you will see two boxes into which the alarm and none alarm paths can be added. There will be no need to click Login Settings as these details have already been defined as described above. Both the Alarm and None-Alarm paths can be found on the Print Tech Document found on Verified Alarms.



VerifiedAlarms Login

General

VerifiedAlarms can be used to receive alarm images triggered by Azimuth. Input your login details for VerifiedAlarms.

☒ Alarm sending is Active

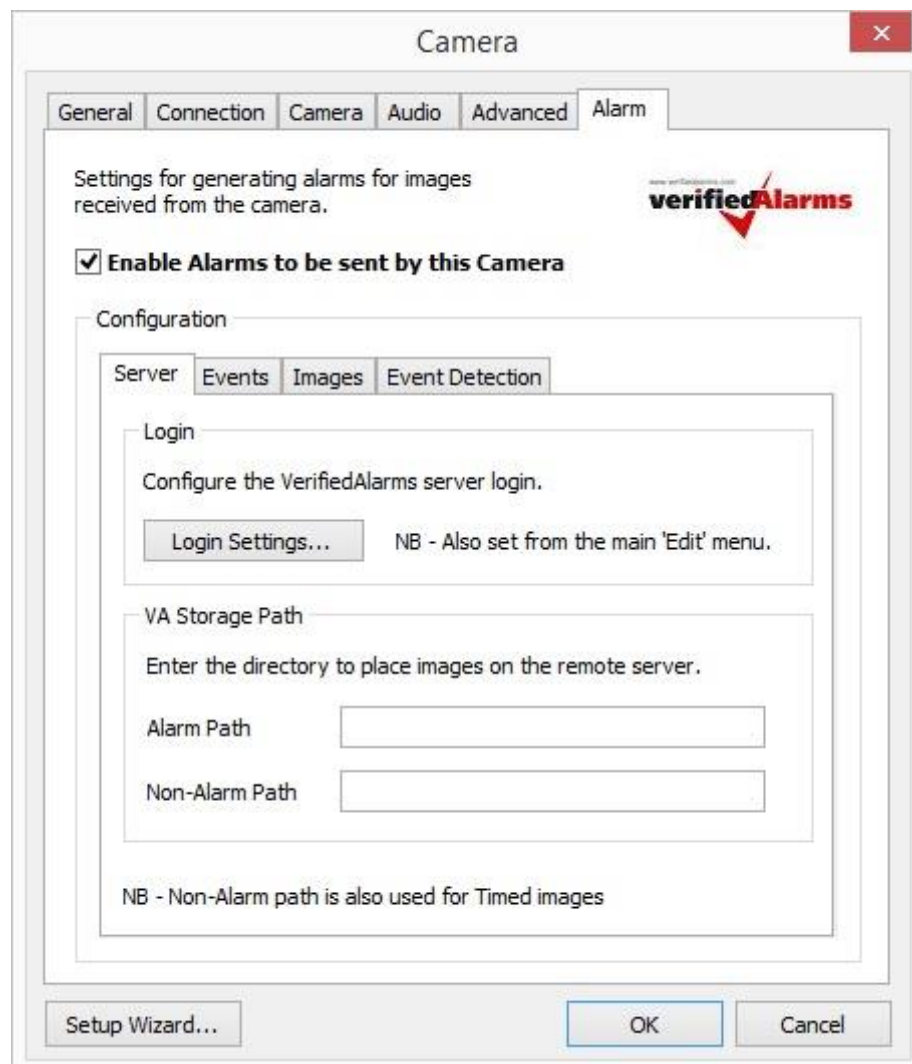
Login Latency iView

Wait Period

Azimuth can delete images from the caches, if the image becomes older than the defined number of minutes, due to delayed transmission.

Maximum wait (minutes) 30

OK Cancel



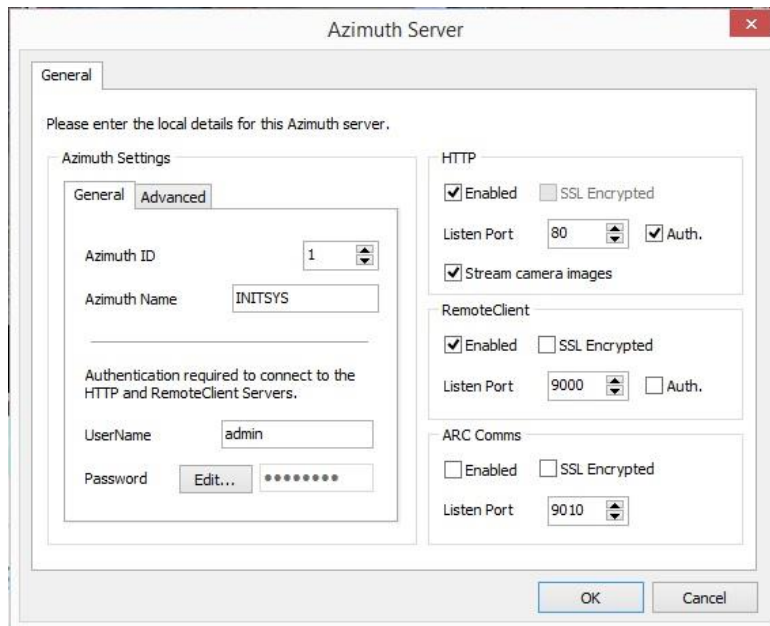
Ensure that Enable Alarms to be sent by this camera is selected otherwise this camera will not send images to the FTP server. In the event section you can define how many images are sent in Alarm and None Alarm events with the images section dealing with how many are sent pre and post alarm. The final tab event detection will take you to the events page which has been discussed in an earlier section of this manual. Once this is complete your Camera should be ready to send to Verified Alarms. When looking at the Camera Viewer an operator can tell when an Image is being correctly sent to a Verified Alarms server by a Verified Alarms logo appearing on the right hand side of the window with a bar showing how many are being sent.

13.0 Connecting to Azimuth Client.

Standard Azimuth machines can be added to a client to be viewed remotely from a machine elsewhere on a site or even in a different country.

Details.

First you must set up the Server Machine (The main Azimuth NVR). Follow Edit → Azimuth Server. A Small window will open where you simply set up the Machines ID, Server name, username/password, and port. These must replicate the settings provided on the client as described below.



Azimuth Server

General

Please enter the local details for this Azimuth server.

Azimuth Settings

General Advanced

Azimuth ID: 1

Azimuth Name: INITSYS

Authentication required to connect to the HTTP and RemoteClient Servers.

UserName: admin

Password: Edit... ..

HTTP

☒ Enabled ☐ SSL Encrypted

Listen Port: 80 ☒ Auth.

☒ Stream camera images

RemoteClient

☒ Enabled ☐ SSL Encrypted

Listen Port: 9000 ☐ Auth.

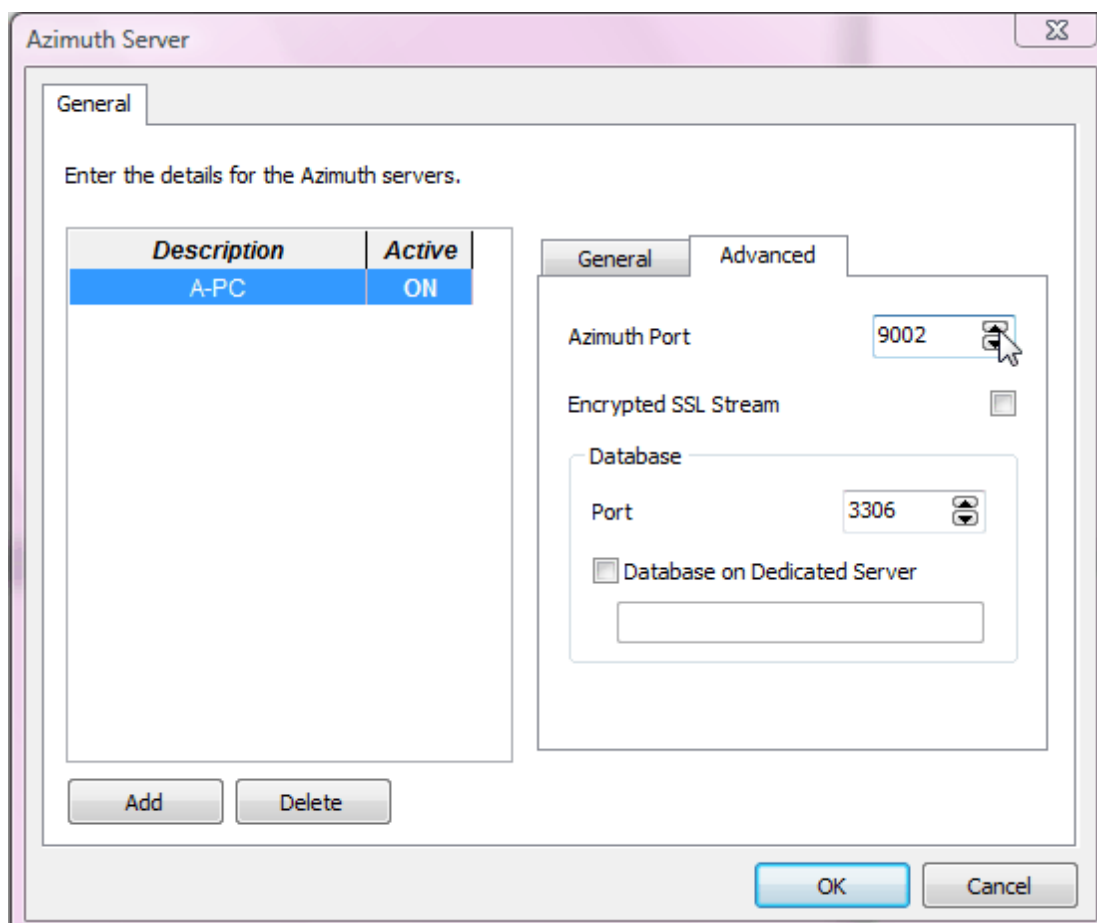
ARC Comms

☐ Enabled ☐ SSL Encrypted

Listen Port: 9010

OK Cancel

Now you must go to the client software itself. In the Client follow File → System → Edit Azimuth Servers and a new window will appear.



Azimuth Server

General

Enter the details for the Azimuth servers.

Description	Active
A-PC	ON

Add Delete

General Advanced

Azimuth Port: 9002

Encrypted SSL Stream ☐

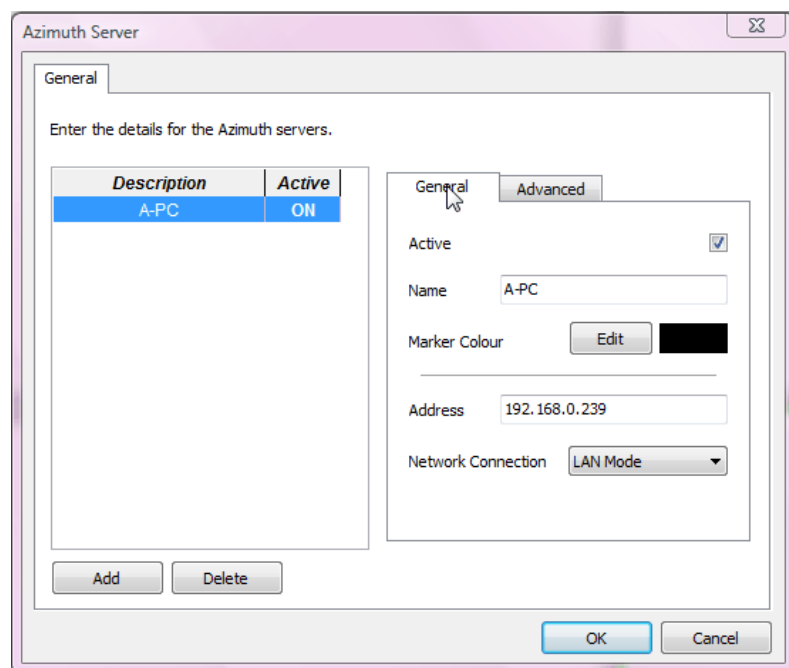
Database

Port: 3306

☐ Database on Dedicated Server

OK Cancel

In the advanced tab you must change the Azimuth Port to the port number you set on the server Machine. Then go to the General Tab and input the Azimuth name exactly how it was on the Server Machine. Also enter the Ip address of the Server system. (Please note this will need to be the remote IP address if the two systems are not on the same network). Ensure that it is ticked as Active and edit the color so that this Server is distinguishable between others on the system. Click OK, and the server should connect.



A video demonstration on how to setup the server connection to the client can be found here:

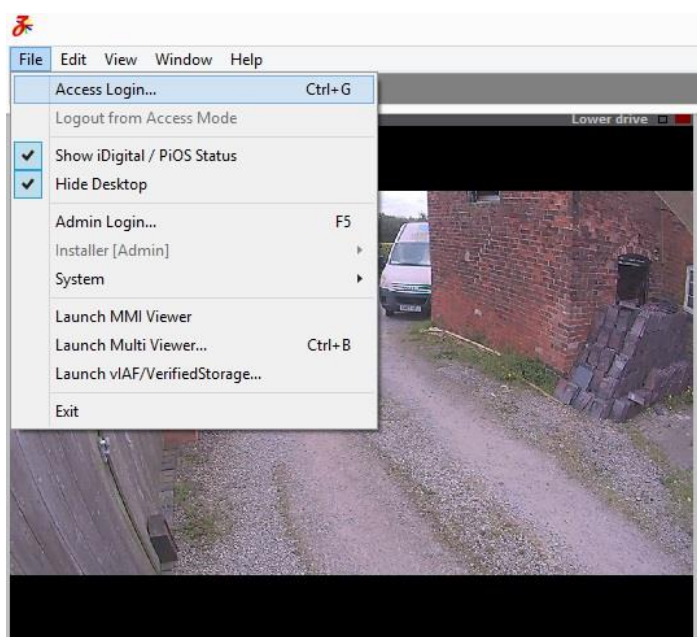
<http://www.azimuthvms.com/tutorials/videos/video/azimuth-enabling-remote-client>

14.0 Miscellaneous.

The basis of this manual explains the more essential parts of the Azimuth software, but there are many more features to cover that might not fall into a certain category. These are covered below following each of option in order.

Details.

Beginning at the File menu.



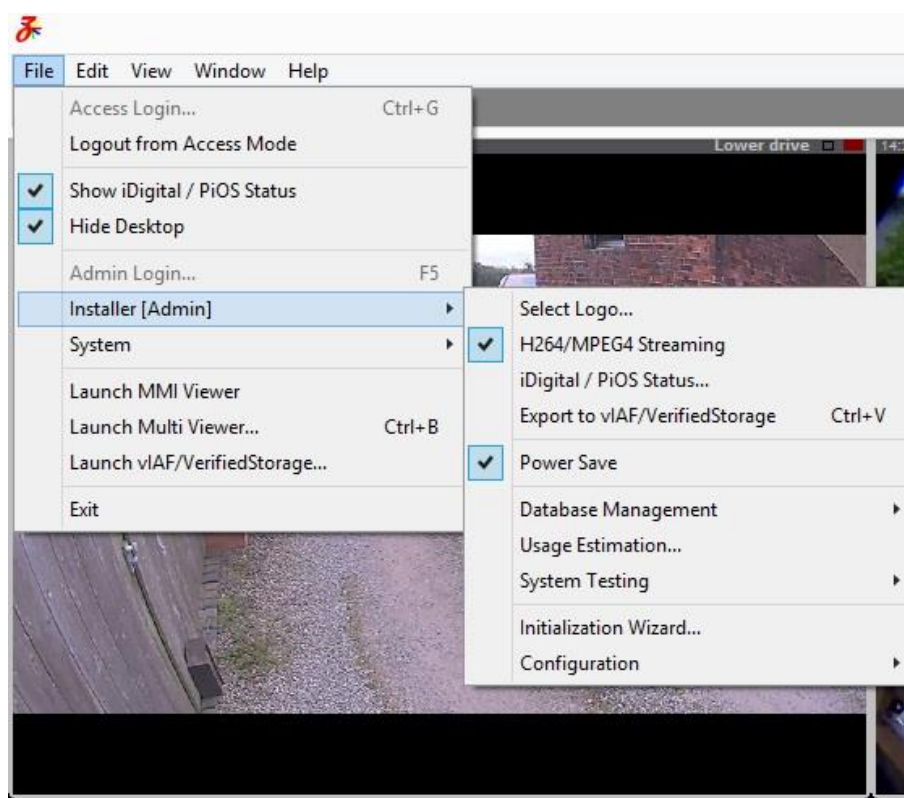
The top two options relate to the current user level. Different levels of user can be defined in the software to prevent or enable operators from either seeing or not seeing certain cameras or settings. How to define what the different levels see of authority to a particular camera can be found in the camera adding section, but to define the different User levels you need to follow Edit → Password.

In this window you will see two sections. One labeled as “Password settings” and one as “Reset Level”. This works in the same way it does if you were to try and change the password on an E-mail account or an online account. You must first, in the top drop down box, select which level you are aiming to alter before inputting the current password (If one is yet to be set it will be blank). You are then below able to add a new password. This will mean that only users with the passwords for the levels they are authorized to view will be able to gain access and the second option down in the file menu is a simple log out from this level and the software will return to its basic level of User.



The third option is covered in the iDigital section and is a simple tick option for whether or not you wish to view the iDigital status LED's in the software's main window. The fourth option will “Hide” the Desktop. As Default Azimuth will appear as only a bar along the top of a window, with any desktop background, including Icons etc., visible. By selecting this option the window will go black, hiding anything behind the Software.

The fifth option is Admin Login. If this is greyed out (Not selectable) then you are already logged into access mode and the Installer Menu below will be available for selection. However, if you are not in Admin mode it will be the opposite way round and upon clicking Admin Login you will be asked for a password to Admin mode (Which unless set as described above, will be blank) and you will therefore be given access to the Installer Menu and some of the important settings in Azimuth.

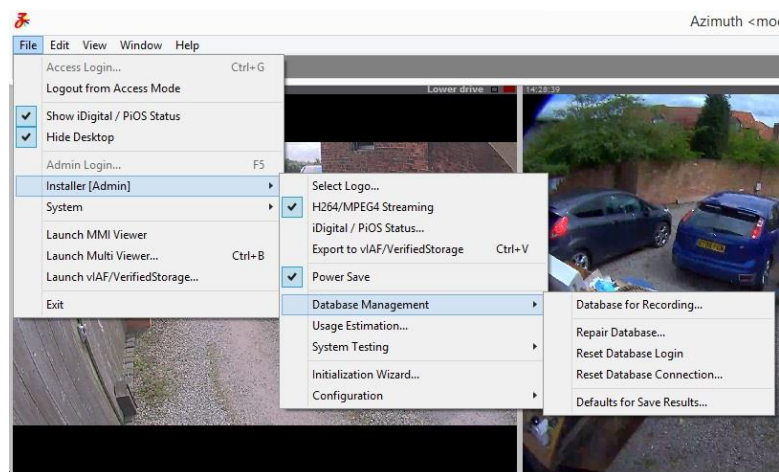


The Installer/Admin menu begins with the Select Logo option. In each of the camera Viewer windows can be seen the Azimuth LTD logo. This can be changed to a logo of the user's choice by selecting this option. It will simply ask for a file to use but this image will be reduced in size automatically and thus the quality will be lowered. The smaller the original image the better the quality. This window informs the user of the Resolution to which the image will be scaled.

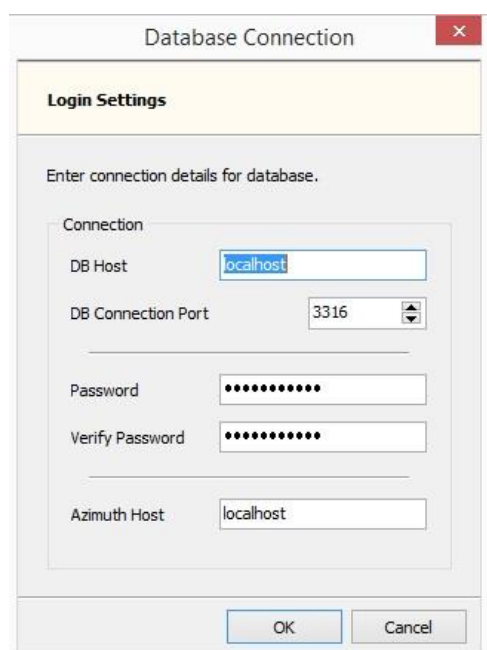
Below this is MPEG4 Streaming. Some Cameras are able to stream in an MPEG4 format, and this option allows for them to do so.

iDigital Status. The option is covered in the iDigital section of this manual.

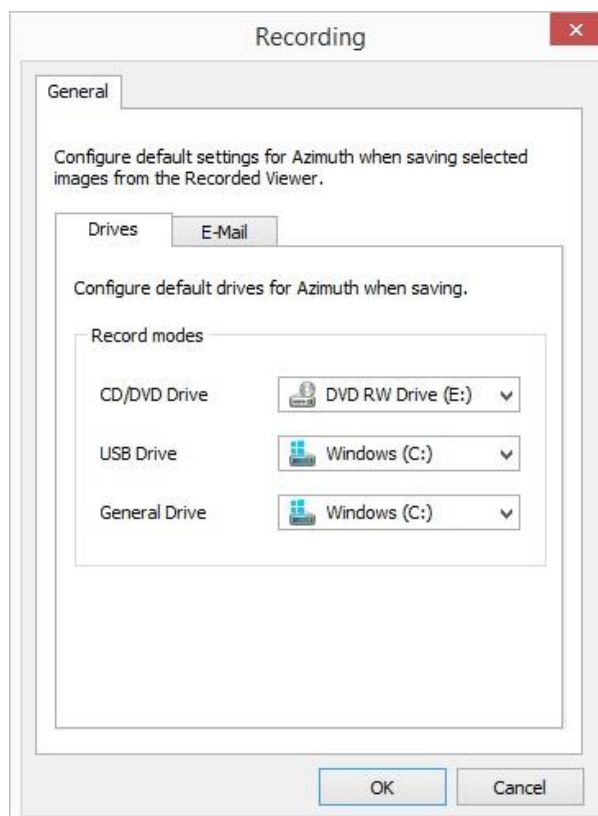
Export to VerifiedStorage is an option that will update settings to your VerifiedAlarms site automatically should new Cameras be added. It is always wise to check these settings once selected.



Database Management. In this section you will find another sub-menu. This area allows you to make changes to the Database, for example the system cleaning. Azimuth can only contain so many images before it runs out of space, and the first option in the sub menu allows you to define how much space is used, on the basis of how much free space is left, before it begins to clean away old images. It asks you for details on where your Maria database is located, usually on the Drive C, but if the Database is not present on that particular machine, that can also be defined. The Repair Database option allows you to check that the tables in the database are OK and are not corrupted as this may cause issues with the saving of details, settings, and images. Reset Database Login will attempt to resets passwords and privileges in the Database if Azimuth is unable to connect to the Database. Reset Database Connection allows you to redefine which Maria Database Azimuth is linked to. When Azimuth was initially installed these details would have been a requirement of the installation in order the recording to work. This section allows for these details to be changed should any of the Maria details have changed.

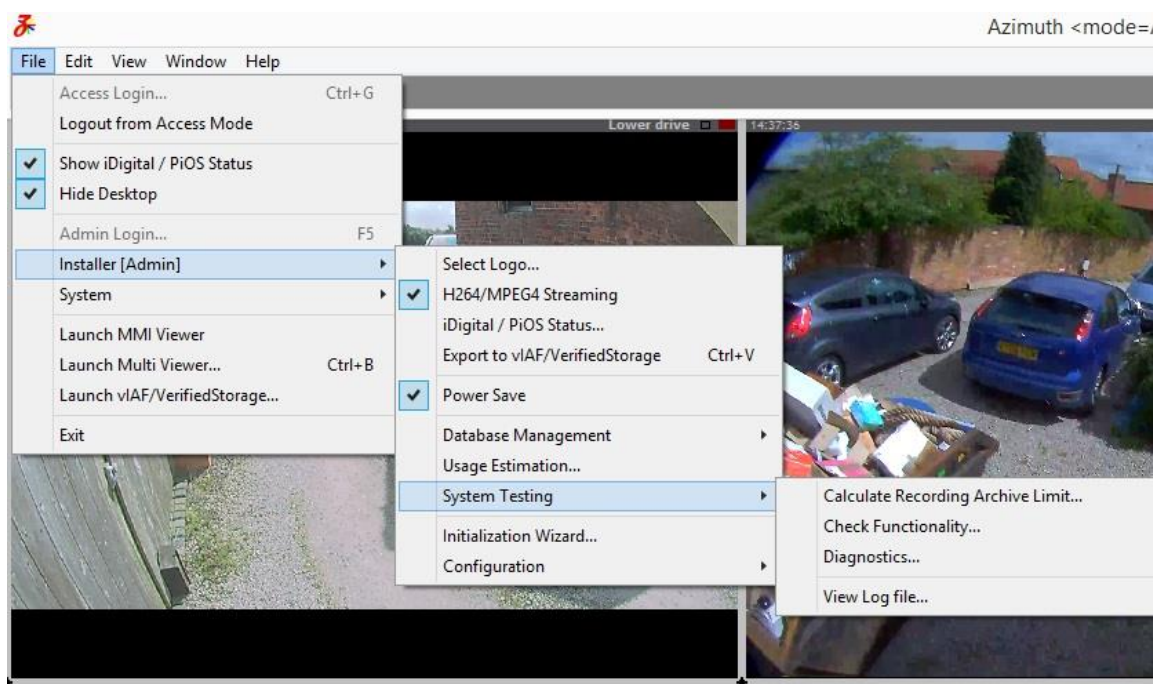


Default for save results is where you select your default save locations for recording images. You can also define a default E-mail address for when recordings are sent Via E-mail.

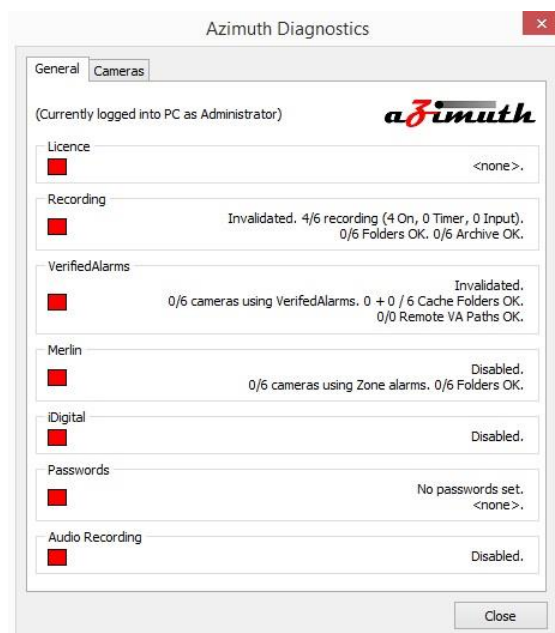


Usage Estimation. This option allows the user to check on the daily recording of a camera and how much space it is likely to use. This can only be on continuous recording as Azimuth cannot possibly predict when a Camera is likely to see Motion and therefore begin recording. It does however provide details on how much recording space has already been used up by that particular camera.

System Testing.



There are 4 options in the System testing sub-menu. The first is to Calculate Recording Archive Limit. This will show you, when selected, whether or not archiving remains and how much. If the system is yet to conduct a forced deletion of Images and thus has a full archive limit, a message will appear informing you to that effect. The Check Functionality section will check which of the Azimuth features are installed and functioning correctly. This is done by means of a quick check showing a list of Azimuth Functions with ticks next to those that are in working order. Any that are now will be shown as Errors. Should an error appear in a section that you intend to use but are unable to fix, Azimuth LTD tech support should be contacted for help in the matter. Diagnostics as shown in the window below, gives details on what parts of Azimuth are currently in use and how. A Secondary tab in the window shows how many cameras are added and gives minor details to their installation, for example in Motion Detection.



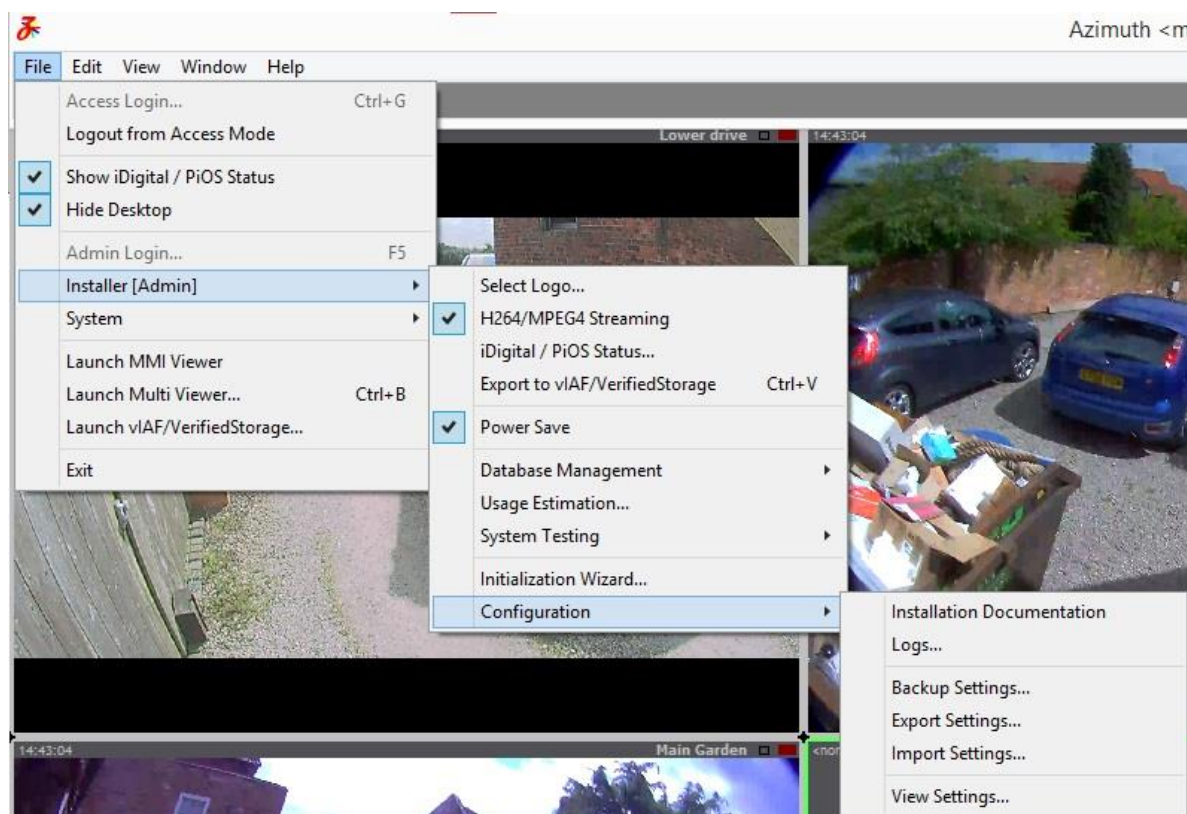
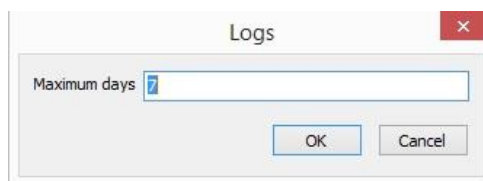
The final option in this sub-section is View Log File. By opening this you will be asked to select a log file, and these can be found on a date basis within the files name. These files simply list every single activity that has taken place of Azimuth. From an operator logging in, to details being changed on a camera, all is logged. It will also log when a Camera connection is lost or regained, and when it records images are sends alarms to Verified Alarms. The systems activity history can be viewed in these logs.

Installation Wizard. This Wizard is intended to be a quick way of setting up many of the aspects of Azimuth already covered in this manual. Each page of the wizard can be found in other sections.

The final section of the Installer/Admin sub-menu is the Configuration Sub-Menu.

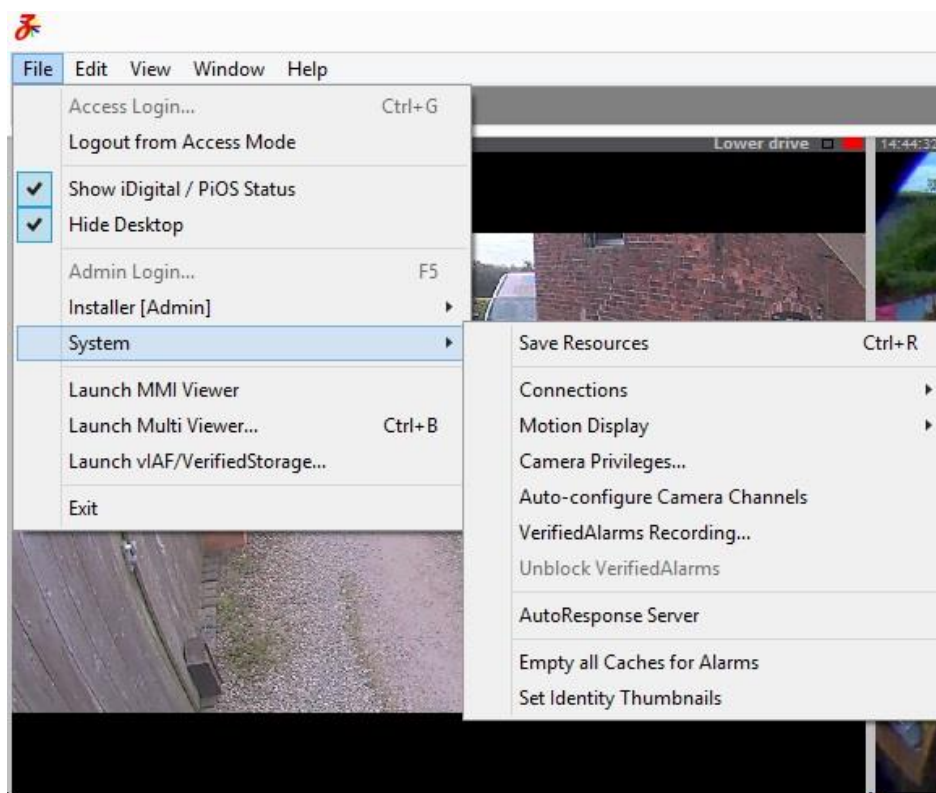
Installation Documentation shows the cameras that have been installed to the System. This is for the purpose of Documentation. It shows the IP address of the camera and their username and passwords etc. This document can be printed, making it handy for engineers who may need to log in to cameras to make changes direct from their laptops. Logs define how many days Azimuth

will create logs for before they are deleted.



Backup Settings will locally backup settings to prevent loss of settings from a computer Crash, whereas Export and Import Settings will save all of the settings of the software to an Ini.File and that can be re-imported or imported to a different system. This enables systems to be formatted and re-installed as they had been operating previously without the need of adding all the settings again. It is recommended that Exports be made every time settings are changed, and backed up to a different machine just in case a system has a fatal error. Note this will not save images. The View Settings option allows you to see the settings as they would be saved in an Ini.File. Minor alterations can be made to the ini that will alter settings but this is not recommended.

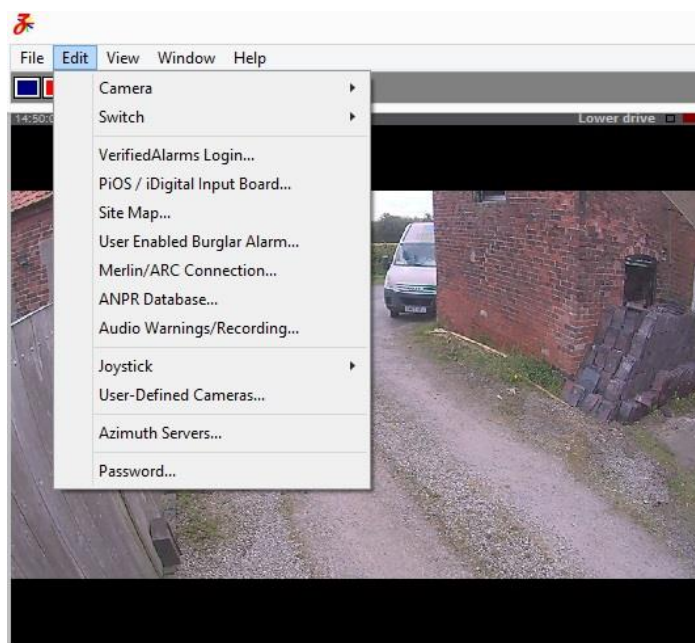
Moving down to Systems another Sub-Menu will appear.



Save Resources is a feature that has been developed as a result of system operating speeds affecting Remote Connections to a system for maintenance purposes. In some cases Azimuth systems can be installed as a “Headless” Unit. This means that it has no screen, Keyboard, or mouse and is simply either logged into remotely or used directly with the Azimuth Client software. If a system is running 20 cameras and an engineer logs into a system via VNC or something similar it can reduce the speed of the connection to the point of being impossible to use. By Selecting Save Resources the camera images will disappear, and Azimuth will not be having to generate the image, thus increasing its operating Speed. Once complete the process can be repeated to allow images to be visible once again. Connections can be started and stopped, basically meaning the connections from the Cameras are either cut off or re-established. This is sometimes handy when a network issue has caused some cameras to drop out and they may only need to be reconnected using this method to re-establish a connection. Camera Privileges is the same feature that you set when adding a camera to enabled is disable viewing to certain user levels. In this section it is more universal, allowing all cameras to be set at the same time. Auto-Configure Camera Channels Tests all the cameras and sets a channel ID if not already allocated. The ID is needed to identify camera in client . VerifiedAlarms Recording allows you to set the frame rate of your verified alarm recording. Like the Camera Privileges section is puts all the cameras into one window allowing you to do it universally in one go, as opposed to individually as you can do when adding or editing a camera. Empty All Caches for Alarms will empty the folders containing Cached images for the purpose of Pre-Post alarm images when sending to VerifiedAlarms.

Launch MMI Viewer will launch the Man-Machine Interface (Covered earlier in this manual) on the camera you have currently selected. If no cameras are selected it will go to the first camera in the list. Launch VerifiedStorage launches the VerifiedStorage window. For details on Verified Storage head to the Verified Storage Section of this manual.

Moving on to the Edit Menu.



The Camera Sub-Menu allows you to Edit, Add, Clone, or Delete a Camera. In order to clone a camera, ensure the camera you wish to clone is highlighted. By Cloning it means it will take all of the installation details from the Camera you have highlighted. This is useful when an multiples of the same model of the camera have been installed that differ only by their IP address. When you select Clone, it will open the same window as it does when you add a camera, with all of the details already added. Simply change the relevant details and it will be added as a new camera.

The Switch Sub-Menu works in exactly the same way as the camera menu, except it will add, Edit, Clone, or delete a camera Switcher. In both the Camera and the Switcher menus you will see an option called Command Menu that will simply open the drop down box in the top left hand of the actual Camera/Switcher Window.

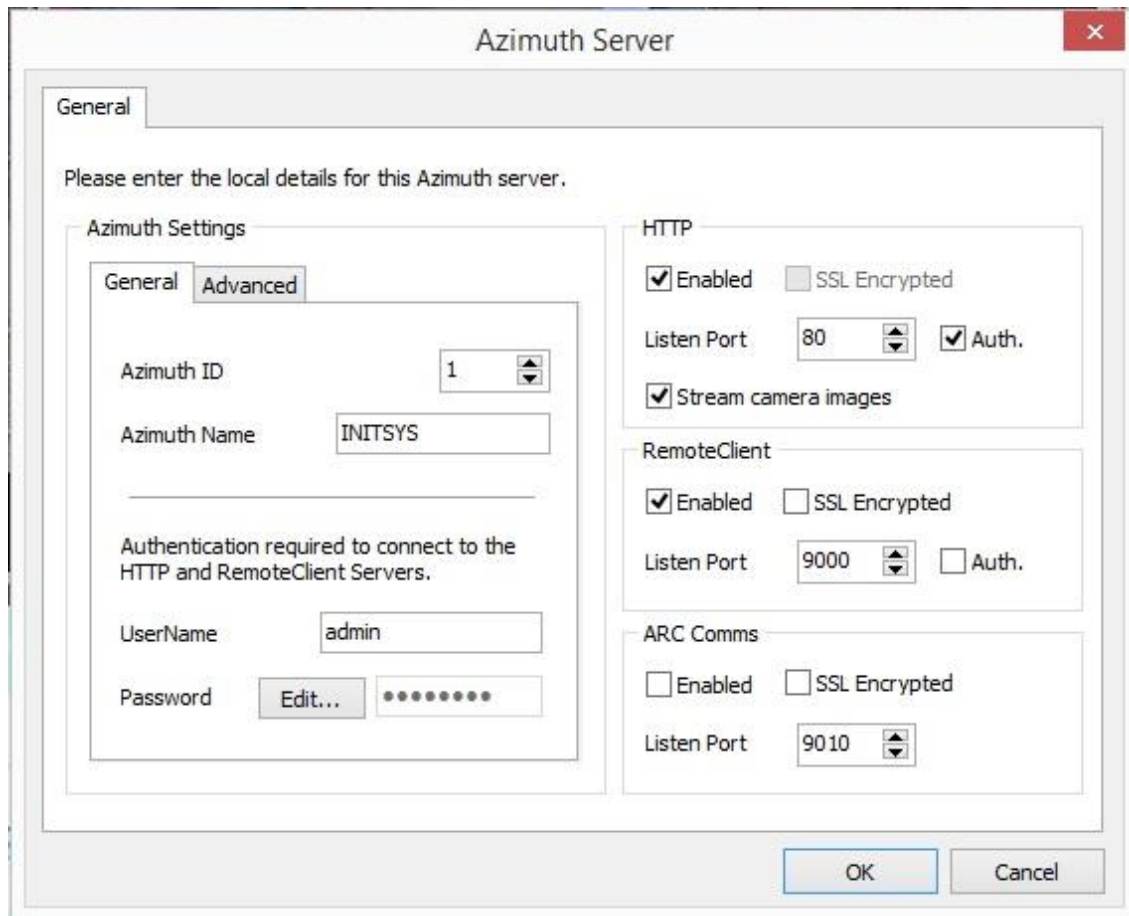
For Information on the Verified Alarms Log In see the Verified Alarms section of this Manual.

For information on the iDigital Input Board and User Enabled Burglar Alarm section see the iDigital section of this manual.

The Merlin/ARC Connection option allows you to add details for a Merlin Connection so that alarms from the iDigital can be sent directly to Merlin with Camera images. Requires use with VerifiedAlarms.

The Joystick option enables you to add a joystick for the purpose of operating a PTZ camera using a Joystick. It must be a USB joystick, with the drivers pre-installed to the PC. User Defined Cameras allows for an operator to add their own camera that might not already be assigned to Azimuth. In order to do this you will need CGI Commands from the Cameras manufacturer.

Azimuth Servers allows you configure the details that are required when setting up Azimuth to be used in conjunction with the Azimuth Client.



Azimuth Server

General

Please enter the local details for this Azimuth server.

Azimuth Settings

General Advanced

Azimuth ID: 1

Azimuth Name: INITSYS

Authentication required to connect to the HTTP and RemoteClient Servers.

UserName: admin

Password: Edit... ..

HTTP

☒ Enabled ☐ SSL Encrypted

Listen Port: 80 ☒ Auth.

☒ Stream camera images

RemoteClient

☒ Enabled ☐ SSL Encrypted

Listen Port: 9000 ☐ Auth.

ARC Comms

☐ Enabled ☐ SSL Encrypted

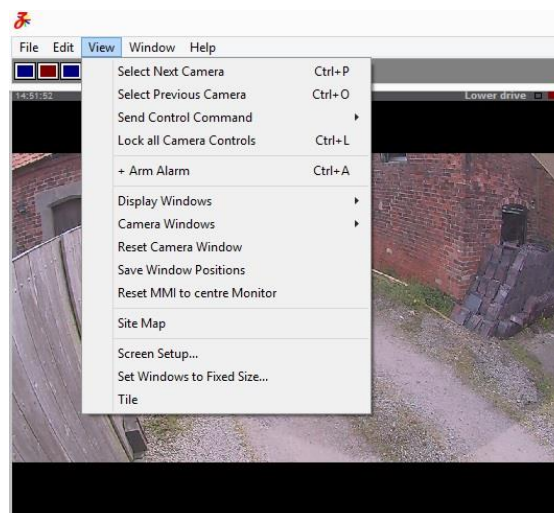
Listen Port: 9010

OK Cancel

Here you define a name of the server and the details on its connection. For detailed instructions on this configuration, please consult the Azimuth Client Manual

Passwords are covered earlier in this section this manual.

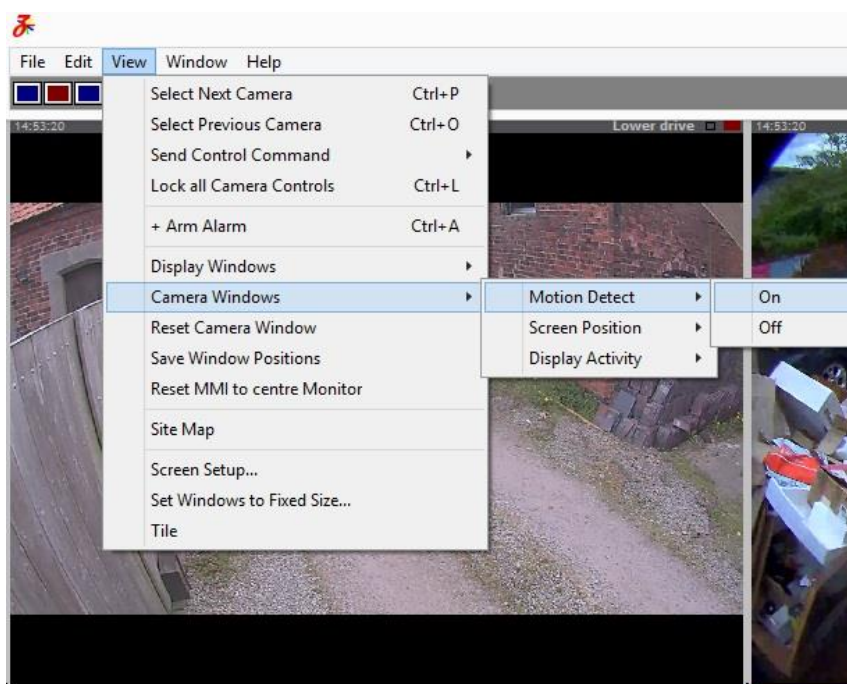
Next is the View Menu.



This menu deals mainly with cameras, their controls and their screen positions.

The first and second in the list are Select Next Camera and Select Previous Camera. Whenever you add a new camera to Azimuth they remain in the order in which you added them. Azimuth will not automatically organize them in Alphabetical or Alphanumerical order. Whenever you select either of the first two options it will simply take you to the next or previous camera in the camera list. (The Window menu will show you the camera list). The Third option, Send Control Command, will open up a smaller sub menu in which you will see a series of Commands. If you have a PTZ camera selected it should then move accordingly to the Commands sent. If the camera doesn't move, it may be because option four, Lock all Camera Controls, is ticked. If so, untick this and the Camera controls will be freed up. +Arm Alarm will set Azimuth to its alarm mode. Settings elsewhere in the setup of Azimuth as explained in other parts of this manual allow for there to be different modes for Alarm events. Alarms can be turned on with this option.

The Next section of the menu deals with the Camera Viewers. Display Windows will open a new sub-menu containing the options Lock and Unlock. This will lock them so that they can no longer be moved by an operator, the Save Window Positions option below will then save their screen location. This is important since if the system was restarted the camera windows may resort back to a previous location if not saved.



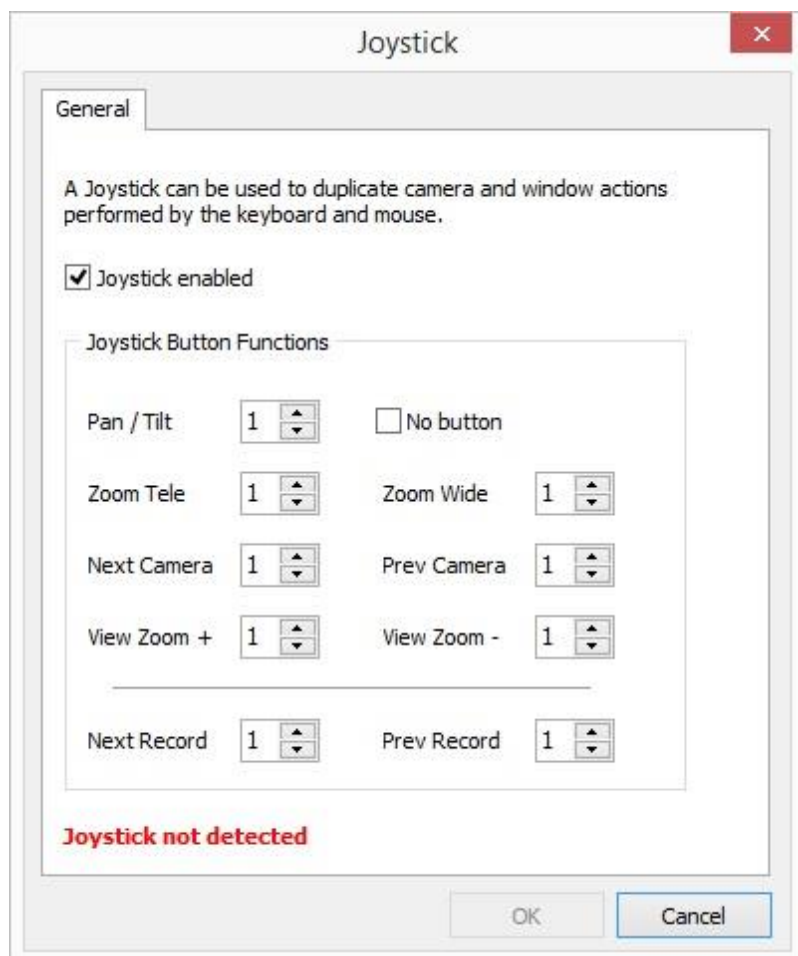
The Camera Windows option will activate a smaller sub-menu. In this section you can turn Motion Detect on and off, lock the screen position (As mentioned above) and determine what is shown on each display window.

Reset Camera Windows and Reset Recording Window will relocate the Camera Viewers and MMI viewers to a default spot should they disappear from view. This could happen when multiple screens are being used and resolution changes may cause a camera viewer or the MMI to disappear. Usually they are relocated to the top left corner and center of the main screen respectively.

Screen Setup... will allow you to set up your camera windows to a certain size and a certain number for Uniformity. This can be done across multiple monitors. A more detailed description on setting up multiple screens can be found at the beginning of this manual. The option below allows you to Set Windows to Fixed Size.. which is good for uniformity of windows and use with video walls. The final option, Tile, will automatically "Tile" an organize any camera windows you have open if they all differ in size and are dotted around a screen.

14.1 Setting up a Joystick.

Joysticks can be configured within Azimuth so that buttons / toggles can be configured to duplicate the actions which can be done using the keyboard and mouse. By going into the Joystick Configure menu you can assign certain buttons on a connected joystick to certain actions within Azimuth.



Actions which can be configured.

- Pan / Tilt
- Zoom Tele
- Zoom Wide
- Next Camera
- View Zoom +
- View Zoom -
- Next Record
- Prev Record

Note: By clicking "No Button" the joystick will recognize the movement of the joystick without a button needing to be pressed before. However without this option being checked, you can configure the joystick so that a certain button needs to be pressed before the movement is sent. This would prevent moving the camera unintentionally.